Legal Aspects of Sweetie 2.0

Schermer, B.W.; Georgieva, Ilina; Van der Hof, Simone; Koops, Bert-Jaap

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

Legal Aspects of Sweetie 2.0

Leiden, October 3, 2016

Authors:
mr. dr. Bart W. Schermer
Ilina Georgieva LLM
Prof. Dr.. Simone van der Hof
Prof. Dr. Bert-Jaap Koops

eLaw@Leiden, Center for Law and Digital Technologies
Leiden University, Faculty of Law

Tilburg Institute for Law, Technology and Society
Tilburg University, Faculty of Law

Table of contents

Acknowledgements

The authors of the present study are indebted to Marcos Salt and Daniela Dupuy, Gregor Urbas, Sofie Royer, Gaëlle Marlier and Charlotte Conings, Paloma Mendes Saldanha, Rowan Hodge, Ines Bojić, Alisdair A. Gillespie, Kaspar Kala, Haykush Hakobyan, Asaf Harduf, Uchenna Jerome Orji, Michael Anthony C. Dizon, Ivan Skorvanek, Andrew Richardson, Matthew Kerr and Eamonn Keane, Jose Agustina and Roberto Valverde, Yong Chul Park, Jonathan Unikowski, Murat Önok and Emre Bayamlıoğlu for sharing their valuable expertise and providing the basis for this comparative legal study – the country reports. A heartfelt thank you to all of them for their contribution and cooperation. We would also like to thank the Danish police for giving us insight into the Danish situation (which is not featured as a country study in this report).

List of abbreviations

AI	Artificial intelligence
ACPA	Anti-Child Pornography Act
ATPA	Anti-Trafficking in Persons Act
BCC	Belgian Criminal Code
CA	Criminal Act
CC	Criminal Code
CCA	Criminal Code Act
CCC	Canadian Criminal Code
CPB	Código Penal Brasileiro (Brazilian Penal Code)
CRA	Child Rights Act
CRC	United Nations Convention on the Rights of the Child
CrCC	Croatian Criminal Code
Cth	Commonwealth
DCC	Dutch Criminal Code
DCCP	Dutch Code of Criminal Procedure
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
ECA	Estatuto da Criança e do Adolescente (Children and Adolescent Statute)
EIO	European Investigation Order
EPC	Estonian Penal Code
EU	European Union
HRC	Human Rights Committee
ICCPR	International Covenant on Civil and Political Rights
IPC	Israeli Penal Code
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
NCA	Nigerian Cybercrimes Act
NPC	Nigerian Penal Code
OP	Optional Protocol
OPSC	Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography
PCC	Polish Criminal Code
PCPSO	Protection of Children and Prevention of Sexual Offences Act
RPC	Revised Penal Code
SCC	Spanish Criminal Code
SOA	Sexual Offences Act
StGB	Strafgesetzbuch (German Penal Code)
TdH	Terre des Hommes
TPC	Turkish Penal Code
UK	United Kingdom
UN	United Nations
USA	United States of America

1 Introduction

1.1 Aims and Challenges

Digital technologies and the Internet may pose risks for the safety and well-being of children. The Internet in particular has created new opportunities for child sexual offenders to find and contact victims, and to sexually exploit them. Sexual predators are active in self-created Internet communities, where they exchange tips and tactics on how to most effectively approach and manipulate children.[1] Perpetrators also use social media platforms and chatrooms to directly engage with victims. This constantly evolving model of sexual exploitation of children is characterised by the exchange of messages with victims via the Internet that typically escalate quickly to sexually-explicit conversations. Once contact has been established, the victim is usually asked or even pressured to undress in front of a webcam, to perform or witness sexual acts, or all of the above. An additional dimension to this problem is the fact that parents or legal guardians may directly be involved in the sexual exploitation of their children. The latter is especially true for families living in developing countries, who prostitute their children as a much needed source of income.

The situation whereby children are engaged in webcam prostitution is generally referred to as webcam child sex tourism. Webcam sex tourism not only causes serious and lasting damage to children[2], it also challenges the effectiveness of criminal investigations, as live webcam performances leave few traces and little evidence that law enforcement can use. Further difficulties arise from the fact that webcam sex tourism often has a trans-border character, which causes jurisdictional conflicts and makes it more difficult to obtain evidence or even launch an investigation.

The Dutch children's rights organization Terre des Hommes ('TdH') was the first NGO to combat webcam child sex tourism by using a virtual character called 'Sweetie'. Sweetie was used to identify offenders in chatrooms and online forums. The Sweetie avatar, posing as a ten-year old Filipino girl, was operated by an agent of the organisation, whose goal was to gather information on individuals who contacted Sweetie and solicited webcam sex. The gathered information was subsequently handed over to the authorities, who thereupon launched investigations in various countries.[3]

The successful implementation of Sweetie 1.0 inspired the further technological development of Sweetie. This time, a technical team commissioned by TdH is engineering an artificial intelligence ('AI') software system, capable of depicting and acting as Sweetie without human intervention in order to not only identify persistent perpetrators, but also to deter first-time offenders.[4]

---

[1] Lovejoy, TP 2007, 'New Playground: Sexual Predators and Pedophiles Online: Criminalizing Cyber Sex between Adults and Minors', p. 312.

[2] Goldstein, RD 1999, *Child abuse and neglect: Cases and materials*, listing the harms to children of premature sexual exposure at p. 144.

[3] Further information on the project known as 'Sweetie 1.0' can be found on www.terredeshommes.nl/en/sweetie-face-webcam-child-sex-tourism. [16 June 2016].

[4] For further information on the second part of the project known as 'Sweetie 2.0' see https://www.terredeshommes.nl/programmas/sweetie-20-webcamseks-met-kinderen-de-wereld-uit. [16 June 2016].

However, the creation of the software raises various challenging legal questions on its application in a law enforcement context. The laws that govern the use of special investigative tools and the role of law enforcement need to be considered. It is precisely this background against which the central question of this legal study takes shape. This report aims to illuminate the existing legal framework of criminal laws and procedures in a number of selected countries in order to determine whether said framework allows for investigative methods such as Sweetie to be used by law enforcement agencies in the fight against webcam child sex tourism.

1.2 Problem statement and research questions

In this report we address the following problem statement:

To what extent is it possible for law enforcement agencies to use Sweetie 2.0 for the investigation and prosecution of webcam sex with minors based on the current criminal law framework (in a selected number of countries)?

The answer to this problem statement may yield the conclusion that the (inter)national criminal law framework may currently not be adequate to combat webcam sex using tools like Sweetie. Therefore, we will also consider the following question:

Which changes to the (inter)national criminal law framework are necessary/desirable in order to facilitate the effective and legitimate use of Sweetie by law enforcement agencies?

To solve this twofold problem statement, we will explore the following research questions:

1.) *How is webcam sex with minors criminalised in selected jurisdictions?*

2.) *To what extent do existing crime descriptions within substantive criminal law apply to virtual victims (i.e., chatbots like Sweetie 2.0)?*

3.) *To what extent does the criminal procedure law framework allow for the (proactive) investigation of webcam sex offences using Sweetie 2.0, taking into account that:*
1. Sweetie 2.0 is an AI that interacts with suspects without direct human control or intervention;
2. A 'fake identity' is used for the AI.

4.) *Are there specific limitations in criminal procedure when it comes to entrapment and what are the consequences of this for using Sweetie 2.0?*

5.) *Which forensic requirements apply to the collection of evidence using Sweetie 2.0?*

Given the global nature of the issue of webcam sex tourism, we will also discuss issues surrounding international investigations and jurisdiction.

1.3 Research Methodology

In this report Sweetie's use will be assessed in the light of the five main legal issues it raises.

In the area of substantive criminal law, these include the application of criminal provisions to virtual victims such as Sweetie, and the criminalisation of preparatory acts and attempts to commit the sexual offences in question. In this context, particular attention will be given to the doctrine of impossible attempts.

In terms of procedural criminal law aspects, we seek to establish whether existing coercive powers can provide a legal basis for the use of Sweetie 2.0. Special investigative powers are usually employed without the suspect's knowledge or consent, which interferes with his/her right to privacy and private life as stipulated in Art. 8 ECHR[5] and Art. 17 ICCPR[6]. In addition, the right to a fair trial as codified in Art. 6 ECHR and Art. 14 ICCPR has to be taken into account when assessing the (proactive) use of artificial intelligence agents in criminal investigations and the thereby triggering defence of entrapment.

We will use the following research methodologies to analyse the use of Sweetie

1.3.1 Desk research and literature study

The basis of the research is desk research and literature study.

1.3.2 Comparative legal analysis

After introducing the international instruments that are relevant for this study, the report continues with the comparative legal analysis. The main goal of the comparative legal analysis is to compare and contrast the legal approaches to dealing with the issue of webcam child sex tourism and the application of Sweetie 2.0. Furthermore, the comparative legal analysis will highlight any issues when it comes to jurisdictional issues related to criminalisation and cross-border investigation.

Given that webcam sex tourism is a global phenomenon a diverse set of countries (in terms of geographical location and legal systems) was chosen for analysis. The following countries were selected for analysis:

Argentina
Australia
Belgium
Brazil
Canada
Croatia
England and Wales
Estonia
Germany[7]

[5] Convention for the Protection of Human Rights and Fundamental Freedoms, CETS no. 194, Rome, 4.XI.1950 (ECHR).
[6] International Covenant on Civil and Political Rights (16 December 1966, entered into force 23 March 1976) 999 UNT 171 (ICCPR).
[7] The information used to assess the German situation reflects on substantive criminal law issues only. Therefore, Germany is not considered in the analysis of criminal procedure.

Israel
Netherlands
Nigeria
Philippines
Poland
Scotland[8]
South Korea
Spain
Turkey
United States

Selection criteria were: geographic spread, type of legal system, exposure to webcam sex tourism and prior experience with Sweetie 1.0.[9] Practitioners and scholars from the selected jurisdictions were asked to prepare a comprehensive report on their respective criminal system and to evaluate it against the research question(s) of the Sweetie project. The authors of the country reports are acknowledged throughout the present study.

1.4 Structure of the report

This study is divided into eight chapters, including the present introduction. The report continues with chapter two, which presents Sweetie, the software behind the avatar, its goals and application. Chapter three discusses the core legal issues raised by Sweetie in terms of substantive criminal law by establishing a baseline of the international law provisions applicable to the matter, and subsequently turns to a comparative analysis of the legal norms that cover webcam child sex tourism in the studied countries. Chapter four does the same with regard to procedural criminal law. Chapter five touches upon the standards of digital forensics relevant for the preservation of data and evidence originating from the cyber domain. Chapter six elaborates on the jurisdictional issues concerning trans-border investigations of webcam sexual assaults of children. An analysis of the restrictions found in the discussed criminal law systems and suggestions on how to adapt the legal frameworks to the challenge of webcam child sex tourism can be found in chapter seven. Chapter eight offers a summary and conclusion of our findings.

2 Sweetie

As a result of the rapid proliferation of devices with cameras, free video chat software (e.g. Skype and Google Hangout), the increase in Internet bandwidth, and the lowering cost of data traffic, people throughout the world now communicate on a daily basis via video. A specific aspect of video chatting is that of a sexual nature: webcam sex.

While webcam sex can take place legally between consenting adults, there are also risks associated with webcam sex, in particular for minors. Risks arise not only because predators

[8] Scotland is officially a part of the United Kingdom, as are England and Wales. However, given the different criminal law system vis-a-vis the rest of the UK, it is listed as a separate country.
[9] Some relevant countries (such as for instance Russia or Kenia) did not make the final selection due to the unavailability of a legal expert in the timeframe of the project.

actively approach unsuspecting minors, but also because a 'cottage industry' of webcam prostitution of minors has emerged, in particular in developing countries. This relatively new phenomenon of webcam child sex tourism has quickly grown into a hidden, but global problem.

To combat webcam sex tourism and raise awareness for the issue, Terre des Hommes developed the Sweetie programme. Sweetie 1.0 was a virtual 10–year old Filipino girl used to identify and expose pedosexuals engaged in webcam sex tourism. Sweetie was operated by a human agent that engaged in conversation with the suspected webcam sex tourist.

While Sweetie 1.0 was extremely successful, one limitation of its design was the human operator. A human operator can only conduct a number of chat conversation at the same time, while real victims receive up to two hundred sex solicitations an hour. To counter this problem TdH has developed a more advanced version of Sweetie: Sweetie 2.0. The main difference with Sweetie 1.0 is that Sweetie 2.0 is no longer operated by a human, but is a now a fully autonomous artificial intelligence that can engage in a meaningful conversation with a suspect.[10] Unlike human operators, the use of this artificial intelligence is in theory infinitely scalable.

2.1 Technology

Sweetie is a virtual minor that engages in conversation with a suspect who has a sexual interest in children with the goal of identifying this suspect. Sweetie is comprised of three main technological elements: 1) three dimensional imagery, 2) a chatbot facility, and 3) an underlying software framework.[11]

2.1.1 3D imagery

The most striking aspect of the original Sweetie was the use of 3D imagery to create a realistic representation of a virtual girl. The realistic animations of Sweetie were designed to make suspects think that they were dealing with a real minor. For Sweetie 2.0 the animations have been further refined. It is important to note that Sweetie's animations do not show any nudity or images of a sexual nature.

2.1.2 Chatbot facility

To eliminate the need for human intervention, Sweetie 2.0 employs AI technology. A chatbot character has been built based on the experiences, work instructions and chat logs from the initial Sweetie project. Using results from the past, the conversation model will simulate as realistically as possible a fictitious 10/11-year-old child.

2.1.3 Software Framework

To use the chatbot functionality for various communication platforms a base has been built that interconnects all software components. These components include, but are not limited to:

- Automated chat functionality for the chatrooms and direct chat;
- Functions to drive the generated imagery;

[10] This type of artificial intelligence is popularly known as a 'chatbot'.
[11] https://tracksinspector.com/blog/ti-software-sweetie-2-0.html. [28 September 2016].

- Management functionality for the chatrooms, characters, chat structure and corresponding question/ answer combinations;
- Storage of all chats and related details;
- Processing of identifiable material from the chats for each chat partner;
- Detection functionality to recognize repeating chat partners, indecent proposals/ or explicit materials;
- Dashboard for graphical presentation of all required actions, chat results, as well as statistics for operational, tactical and strategic insight;
- Reporting module to confront potentially offending chat partners with their own behaviour and chat phrases. This module will also follow up with relevant advice, deterrent warnings and/ or possible threat of identification, based on the findings of current academic research for the project.

The chat logs are stored and exchanged data are processed per chat to a profile for each chat partner. This profile can ultimately be used to identify repetitive patterns. All chat reports and extracts of chats are logged in a universally accepted standard which facilitates the exchange of cases. This will take into account generic storage methods used by various national and international (investigation) agencies such as Interpol and Europol in order to simplify matching with other (online) child abuse cases.

3 Substantive criminal law

Sweetie is an investigative tool that enables law enforcement to engage with sexual predators and interact with them. If law enforcement is to use Sweetie as an investigative method, this means that the actual behaviour under investigation (i.e., interacting with Sweetie) must be deemed criminal behaviour. If this is not the case, then it will be much harder, if not impossible to prove that the suspect committed or attempted a criminal act. This in turn will make it more difficult to justify the use of Sweetie as an investigative method.

In this chapter we explore whether and how (an attempt) to interact with Sweetie in a sexually oriented way is criminalised in the various jurisdictions under investigation. To this end we first consult the international law instruments to establish a 'baseline' of criminal behaviour and then explore specific substantive law issues in relation to webcam sex in general and webcam sex with an avatar such as Sweetie in particular.

3.1 Criminalisation of abuse of minors and international harmonisation

In most, if not all jurisdictions worldwide, sexual abuse of minors is criminalised. Different forms of abuse are criminalised in national criminal law. Apart from criminalisation at the national level, there is also international harmonisation when it comes to the protection of minors and the criminalisation of abuse of minors.

At a global level the protection of minors is codified in different international law instruments. For the purpose of this report we will explore four particularly relevant international law instruments: 1) the UN Convention on the Rights of the Child (CRC),[12] and 2) the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OPSC),[13] 3) the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)[14] and, 4) the Council of Europe Cybercrime Convention.[15,16]

3.1.1 UN Convention on the Rights of the Child

The United Nations Convention on the Rights of the Child (CRC) is an international treaty that sets out the civil, political, economic, social, health and cultural rights of children. At the

[12] Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC or UNCRC), available at: http://www.ohchr.org/en/professionalinterest/pages/crc.aspx. [13 June 2016].
[13] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (adopted on 25 May 2000, entered into force 18 January 2002) A/RES/54/263, available at: http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx. [13 June 2016].
[14] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS 201, Lanzarote, 25.X.2007 (Lanzarote Convention).
[15] Council of Europe Convention on Cybercrime, CETS No.185, Budapest, 23.XI.2001 (Budapest Convention), available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf. [13 June 2016].
[16] Both the Lanzarote Convention and the Cybercrime Convention are Council of Europe instruments. In the European Union Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children, and child pornography is also applicable. Given the more global remit of the Council of Europe instruments, we will not discuss Directive 2011/93/EU further in the context of this report.

moment of writing there are 196 countries party to the treaty.[17] The United States is the only member of the UN that has not ratified the document.

The fundamental idea of the CRC is that every child, every human being below the age of eighteen years, is born with fundamental freedoms and the inherent rights of human beings. Moreover, the CRC recalls that children are entitled to special care and assistance because of their vulnerability.[18] According to the preamble children need to grow up 'in a family environment, in an atmosphere of happiness, love and understanding.'[19] Article 20 of the CRC, for example, states that a child temporarily or permanently deprived of his or her family environment shall be entitled to special protection and assistance provided by the state. Furthermore, General Comment 13 to the CRC underlines the importance that every child's life must be free from all forms of violence.[20]

While the CRC does not criminalise specific acts against the well-being of children, several articles put a positive obligation on the states to protect children against sexual abuse and exploitation. Article 19 and Article 34 are particularly relevant in this regard:

> ***Article 19***
> *States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child.*
>
> ***Article 34***
> *States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:*
> *(a) The inducement or coercion of a child to engage in any unlawful sexual activity;*
> *(b) The exploitative use of children in prostitution or other unlawful sexual practices;*
> *(c) The exploitative use of children in pornographic performances and materials.*

3.1.2 Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography

The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OPSC) has been signed by 182 state parties to this date, yet no more than 173 have ratified it.[21] The protocol is intended to achieve the purposes of the articles in the CRC. For example, Article 1 states that parties are to protect the rights and interests of child victims of trafficking, child prostitution, child pornography and child labour.

---

[17] https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11&chapter=4&lang=en. [18 May 2016].
[18] UNCRC, Preamble, paras 4 and 9.
[19] UNCRC, Preamble, para 6.
[20] Committee on the Rights of the Child 2011, *General comment No. 13: The right of the child to freedom from all forms of violence*, CRC/C/GC/13.
[21] https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11-c&chapter=4&lang=en. [18 May 2016].

Article 2 (broadly) defines the criminal acts of sale of children, child prostitution and child pornography:

> *For the purposes of the present Protocol:*
>
> *(a) Sale of children means any act or transaction whereby a child is transferred by any person or group of persons to another for remuneration or any other consideration;*
>
> *(b) Child prostitution means the use of a child in sexual activities for remuneration or any other form of consideration;*
>
> *(c) Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.*

The OPSC obliges states to criminalise these practices. Finally, the protocol sets international standards for mutual assistance in investigations, confiscation of assets and extradition.

3.1.3 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)

The Lanzarote Convention is a Council of Europe Convention aimed at combating sexual exploitation and abuse of minors. The purposes of the Lanzarote Convention are defined in Article 1:

- Prevent and combat sexual exploitation and sexual abuse of children;
- Protect the rights of child victims of sexual exploitation and sexual abuse;
- Promote national and international co-operation against sexual exploitation and sexual abuse of children.

The treaty obliges parties to pass laws that criminalise any practice that is in conflict with these purposes, for instance child pornography. All Member States of the Council have ratified the treaty.

We will use the Lanzarote Convention as a basis for our discussion of substantive criminal law as it provides the most complete inventory of crimes related to minors.

3.1.4 Council of Europe Cybercrime Convention

Being the first in its kind, the Convention on Cybercrime pursues a common criminal policy aimed at the protection of society against crimes committed via the Internet and other computer networks.[22] The treaty fosters fast and effective international cooperation, harmonisation of domestic criminal law in the area of cybercrime and the provision of domestic criminal procedural law powers necessary for the investigation and prosecution of such crimes. The

[22] Convention on Cybercrime, Preamble, para 8.

Convention contains provisions on a wide variety of crimes, such as violations of network security, computer related fraud and child pornography.

Thus far, 49 states have ratified the Cybercrime Convention.[23] Parties to the treaty are not only Member States of the Council of Europe. The treaty is also ratified by Australia, Canada, The Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka and the United States. Relevant for the purpose of this study is that the Cybercrime convention criminalises offences related to child pornography (Article 9).

3.1.5 International harmonisation in the area of abuse of minors

The table below specifies which of the countries under investigation in this study have signed and ratified the international law instruments described above.

Table 1: International harmonisation in the area of abuse of minors

	UN Convention on the Rights of the Child (CRC)	Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OPSC)	Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)	Council of Europe Cybercrime Convention
Argentina	X	X	-	-
Australia	X	X	-	X
Belgium	X	X	X	X
Brazil	X	X	-	-
Canada	X	X	-	X
Croatia	X[24]	X	X	X
England and Wales	X	X	S (Signed, not ratified)	X
Estonia	X	X	S	X
Germany	X	X	X	X
Israel	X	X	-	X
Netherlands	X	X	X	X
Nigeria	X	X	-	-
Philippines	X	X	-	-
Poland	X	X	X	X
Scotland	X (UK)	X (UK)	S (UK)	X (UK)
South Korea	X	X	-	-
Spain	X	X	X	X
Turkey	X	X	X	X
United States	S	X	-	X

[23] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201/signatures. [18 May 2016].
[24] Signed by Yugoslavia, ratified by Croatia.

3.2 Criminalisation of webcam sex with minors

This section reviews the criminal law offences potentially applicable to sexual abuse of minors via webcam. It does so by summarising the provisions focusing on the key types of behaviour regularly occurring in webcam abuse. It then turns to evaluate whether and how said provisions apply to virtual minors such as Sweetie.

3.2.1 International harmonisation

What we can deduct from table 1 is that while all countries under investigation in this study have signed and ratified the CRC and the OPSC, not all countries have signed the Lanzarote Convention, which provides the most complete inventory of criminal offences related to the abuse of minors. This may pose a problem when it comes to the international harmonisation of the criminalisation of webcam sex, given that the OPSC does not specifically define or criminalise certain types of child exploitation such as webcam sex and grooming.

Criminal behaviour aimed at minors that does not qualify as prostitution or as child pornography is, for instance, not covered by the OPSC. This means that crimes such as webcam sex, grooming and the corruption of children are not fully harmonised throughout the jurisdictions under examination.

Furthermore, it may also mean that webcam sex, grooming and the corruption of children are not criminalised at the national level. Though when it comes to the topic of this research (webcam sex with minors) we have not found any proof of this. All jurisdictions that did not sign the Lanzarote Convention have still criminalised webcam sex with minors in national law, in one way or another (see table 3).

3.2.2 Relevant crime descriptions

The international law instruments described above and the national criminal laws of the different countries contain a number of broadly formulated crime descriptions that may or may not cover webcam sex with minors.

Depending on the exact form and circumstances of the act, the offences listed below may come into view when a person is interacting with a minor though a webcam for the purpose of sexual gratification. For the sake of good order we use the articles from the Lanzarote Convention as a framework for discussion. The relevant articles are:

- Article 18. Sexual abuse
- Article 19. Offences concerning child prostitution
- Article 20. Offences concerning child pornography
- Article 21. Offences concerning the participation of a child in pornographic performances
- Article 22. Corruption of children
- Article 23. Online solicitation of children for sexual purposes

3.2.2.1 Sexual abuse

Sexual abuse may cover a range of sexual activities that take place between the perpetrator and the minor, such as rape, assault and the commission of lewd/lascivious acts. Article 18 of the Lanzarote Convention defines sexual abuse as:

> *a. engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities;*
> *b. engaging in sexual activities with a child where: – use is made of coercion, force or threats; or – abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or – abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence.*

Paragraph 1a criminalises engaging in sexual activities with a person who has not reached the age at which it is allowed to engage in sexual activities with him or her. This age is established in domestic law:

> *2. For the purpose of paragraph 1 above, each Party shall decide the age below which it is prohibited to engage in sexual activities with a child.*

Paragraph 1b criminalises engaging in sexual activities with a child where use is made of coercion, force or threats, or when this person abuses a recognised position of trust, authority or influence.

All of the countries under investigation have provisions in their domestic law that criminalise sexual abuse of minors. In the Lanzarote Convention the term 'sexual activities' has not been further defined. The negotiators preferred to leave it to the States to further define the meaning and scope of the term.[25] In the domestic law of the countries under investigation, 'sexual activities' generally cover acts whereby there is direct physical contact (including by force, under threat or through other forms of coercion) between the perpetrator and the victim, such as rape and assault. A position of trust, authority or influence over the minor is an aggravating circumstance, which generally carries higher penalties.

3.2.2.2 Offences concerning child prostitution

Child prostitution covers a number of criminal acts whereby a minor is used for sexual activities in exchange for some form of remuneration. Article 2 paragraph b of the OPSC defines child prostitution as:

> *(...) the use of a child in sexual activities for remuneration or any other form of consideration.*

Article 19 paragraph 2 of the Lanzarote Convention defines child prostitution as:

[25] *Explanatory report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. CETS 201*, para 127.

(...) the fact of using a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment, regardless if this payment, promise or consideration is made to the child or to a third person.

Offences concerning child prostitution
1. Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalised:
a. recruiting a child into prostitution or causing a child to participate in prostitution;
b. coercing a child into prostitution or profiting from or otherwise exploiting a child for such purposes;
c. having recourse to child prostitution.

Criminal liability is extended to both the person(s) prostituting the minor and the customer(s). In relation to the topic of this research, this article is of particular importance. In most cases of webcam sex with minors, a minor from a developing country is forced or coerced by a third party (parents, criminals) to participate in a webcam session with a perpetrator (the 'webcam sex tourist'). This webcam sex tourist generally wants to watch (and indirectly participate in) a pornographic performance involving a minor in exchange for money.

Given the broad definition of 'sexual activities' there are no a priori limitations to applying this article in the context of webcam sex tourism.

3.2.2.3 Offences concerning child pornography

Offences concerning child pornography are also highly relevant in the context of webcam sex with minors and webcam sex tourism, given that the images streamed and captured via the webcam will generally qualify as child pornography.

Child pornography is criminalised in the OPSC, the Lanzarote Convention and the Cybercrime Convention.

The OPSC uses the following definition of child pornography:

Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.

In the Lanzarote Convention child pornography is defined as:

(...) any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes.

Finally, according to the Cybercrime Convention:

the term 'child pornography' shall include pornographic material that visually depicts:
a) a minor engaged in sexually explicit conduct;
b) a person appearing to be a minor engaged in sexually explicit conduct;
c) realistic images representing a minor engaged in sexually explicit conduct.

In the international law instruments at hand both the production and consumption of child pornography is criminalised. The Lanzarote Convention lists the following acts as criminal:

a. producing child pornography;
b. offering or making available child pornography;
c. distributing or transmitting child pornography;
d. procuring child pornography for oneself or for another person;
e. possessing child pornography;
f. knowingly obtaining access, through information and communication technologies, to child pornography.

When it comes to illegal webcam sex, sub c and f are of particular interest. Before the advent of webcam sex, most of the child pornography was either distributed by means of physical carriers (photos, magazines) or obtained digitally and subsequently stored on local media such as hard drives and DVDs. In these cases procurement and possession of child pornography could be proven more easily. With webcam sex, however, by default there is no local storage of the streamed data, unless the offender records the stream or takes screenshots. The ephemeral nature of this type of child pornography consumption means that procurement and possession is difficult, if not impossible to prove. Therefore, article f criminalises the access to child pornography in itself. As such, webcam sex with minors may also fall under the heading of (attempting) to access child pornography.[26] On the 'production side' making a webcam sex stream available may fall under the heading of sub c (transmitting child pornography).[27]

Virtual child pornography
Apart from actual child pornography, many countries also criminalise the production, sale, possession of and access to 'virtual' child pornography. Virtual child pornography refers to images whereby it realistically *appears* that a minor is engaged in sexually explicit conduct. This is particularly relevant for Sweetie, which is a virtual minor that may appear to be engaged in sexually explicit behaviour.

Both the OPSC and Lanzarote Convention use broad definitions of child pornography that may also include images of virtual minors engaged in sexually explicit conduct or the computer-generated depiction of a child's sexual organs for primarily sexual purposes. After all, they see to 'any representation' or 'any material that visually depicts', which may include computer-

[26] Please note that paragraph 4 of Article 2 OSPC gives countries the possibility to not apply paragraph 1f in national law.
[27] In Canada for instance, subs. 163.1 (4.2) of the Canadian Criminal Code criminalises the viewing of webcam performances by attaching liability to those who knowingly access child pornography by knowingly causing child pornography to be viewed by or transmitted to himself or herself. Following the interpretation of the Supreme Court, Art. 383*bis* § 2 of the Belgian Criminal Code also penalises knowingly and without a right accessing child pornographic images through information and communication technologies.

generated representations. However, while the Lanzarote Convention clearly intends to include it within the definition's scope (see Art. 20 paragraph 3), for the OPSC this is not evident. One could also argue, therefore, that virtual child pornography is not explicitly referred to, it is not included in the OSPC definition.

The Cybercrime Convention, in contrast, does use an explicit reference to virtual child pornography, as long as the images are realistic:

> *'... the term 'child pornography' shall include pornographic material that visually depicts:*
> *(...)*
> *c) realistic images representing a minor engaged in sexually explicit conduct.'*

In the Explanatory Memorandum to the Cybercrime Convention virtual child pornography is further described as:

> *'images, which, although 'realistic', do not in fact involve a real child engaged in sexually explicit conduct. This latter scenario includes pictures which are altered, such as morphed images of natural persons, or even generated entirely by the computer.'*[28]

Under both the Lanzarote Convention and the Cybercrime Convention it is optional to criminalise virtual child pornography (see Article 20 paragraph 3 and Article 9 paragraph 4 respectively).

[28] *Explanatory Report to the Council of Europe Convention on Cybercrime*, para 101.

Table 2: Criminalisation of (virtual) child pornography		
	Child pornography	Virtual child pornography
Argentina	X	-
Australia	X	X[29]
Belgium	X	X
Brazil	X	-[30]
Canada	X	X[31]
Croatia	X	X
England and Wales	X	+/-[32]
Estonia	X	X
Germany	X	X[33]
Israel	X	-
Netherlands	X	X
Nigeria	X	X
Philippines	X	X
Poland	X	+/-[34]
Scotland	X	+/-[35]
South Korea	X	-
Spain	X	X[36]
Turkey	X	X
United States	X	X

3.2.2.4 Offences concerning the participation of a child in pornographic performances

Article 21 of the Lanzarote Convention criminalises pornographic performances with minors:

[29] McEwewn v Simmons & Anor [2008] NSWSC 1292 at paras 38-39, confirming convictions for possession of virtual child pornography under both Commonwealth and State legislation. For more on the matter see Urbas, G, *Substantive and procedural legislation in Australia to combat webcam-related child sexual abuse* (Australian report), p. 19.

[30] Article 241-E of the ECA refers to 'real or simulated' sexual activities. However the official interpretation of the provision is understood as implying the participation of *real* minors in the simulated activities and not of virtual victims.

[31] It appears that virtual child pornography, although not explicitly regulated, is criminalized as a matter of statutory interpretation of the definition given to the term, 'child pornography' at s. 163.1 of the Canadian Criminal Code.

[32] May fall under the heading of 'pseudo-photograph' of a child but if it does not, virtual images are also classed as child pornography under a different piece of legislation. They would be known as prohibited images of children (see country report on England and Wales).

[33] Virtual child pornography is covered by §184b (1) no. 2 and (3) StGB and covers realistic depictions of children that an average informed person could not tell apart from the depictions of real children.

[34] Child pornography is not further defined in Polish law. However, a broad interpretation of the term should be taken; see Skorvanek, I, *Substantive and procedural legislation in Poland to combat webcam-related child sexual abuse* (Polish report).

[35] May fall under the heading of 'pseudo-photograph', but not entirely clear (see Scotland country report).

[36] Article 189.1d) speaks of images that 'appear to be of a child' and of 'realistic' images. In general, based on the letter of the law, virtual child pornography is penalised too.

(...) a. recruiting a child into participating in pornographic performances or causing a child to participate in such performances;
b. coercing a child into participating in pornographic performances or profiting from or otherwise exploiting a child for such purposes;
c. knowingly attending pornographic performances involving the participation of children.

Article 21 Paragraph 1 sub a and b focus on those organising the performance, whereas paragraph c focuses on the attendance of such performances.

The OPSC does not specifically criminalise pornographic performances with a minor, but these might be covered by the broader notion of child prostitution:

(...) (b) Child prostitution means the use of a child in sexual activities for remuneration or any other form of consideration;

The Cybercrime Convention does not cover pornographic performances, although the recording of broadcasting of such a performance will be considered producing and distributing, offering, and/or transmitting child pornography.

A webcam stream in which a minor performs sexual activities can be considered a pornographic performance. The question though is if attendance of such a performance at a distance is covered in the crime description. Whether this is the case is dependent on the domestic law of the countries under investigation. The Lanzarote Convention does specifically address this issue in the explanatory report, but leaves it to the contracting states to determine whether or not they wish to include webcam sex:

Depending on States, this provision may also cover the situation of persons who are spectators of pornographic performances involving the participation of children through such means of communication as webcams.[37]

3.2.2.5 Corruption of children

The corruption of children is a specific offence criminalised in the Lanzarote Convention. The OPSC or the Cybercrime Convention do not cover it. Article 22 of the Lanzarote Convention criminalises:

(...) the intentional causing, for sexual purposes, of a child who has not reached the age set in application of Article 18, paragraph 2, to witness sexual abuse or sexual activities, even without having to participate.

In the context of webcam sex this offence is relevant as it may cover those situations whereby:

[37] *Explanatory report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.*

1) the perpetrator performs sexual activities in front of the webcam (e.g., masturbation).[38]

2) the perpetrator tries to corrupt the minor, for instance by sending pictures of sexual activities to the minor or by promoting sexual activities using online chat functions.

Given that it is possible to (video)chat with Sweetie, it is very well possible that these offences may also be committed by suspects alongside other offences. With Sweetie 1.0, suspects did indeed perform sexual activities in front of the webcam in ways that amounted to the corruption of children.

Furthermore, in some criminal systems a sexually-charged chat with a (virtual) minor may be sufficient to meet the threshold of child corruption. This is the case, for instance, in Australia, where the suspect does not necessarily have to transmit imagery to the minor to bring about the corruption.[39] The law speaks of 'indecent communication', whereas just the chat can meet this threshold provided that the communication language goes against the moral standards of ordinary people. In a similar vein, it appears that the Polish legislator has opted for a rather broad understanding of the term 'pornography', which would allow to see the indecent chat as pornographic material as well.

3.2.2.6 Online solicitation of children for sexual purposes (grooming)

Online solicitation of children for sexual purposes, more commonly referred to as 'grooming' is only criminalised in the Lanzarote Convention:

> *Each Party shall take the necessary legislative or other measures to criminalise the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a, or Article 20, paragraph 1.a, against him or her, where this proposal has been followed by material acts leading to such a meeting.*

Grooming commonly takes place via either online chat or webcam, and as such it is related to the subject matter of our research. However, webcam child sex tourism focuses on having sexual contact through the webcam, not in physical proximity. As grooming is defined as proposing to meet (in real life), it is a form of real-life child sex tourism. Although perpetrators chatting with Sweetie may also propose a real-life meeting, this is not the primary focus of the types of cases we study. Having said that, Sweetie 2.0 may of course also be used in a national setting to lure groomers.

3.3 Issues pertaining to the criminalisation of webcam sex with minors

Having reviewed the different types of crime descriptions above we may conclude that at the international level there are different options for states to criminalise webcam sex (tourism)

[38] Exposing oneself in front of a minor and/or masturbating may also be criminalised in domestic law under the header of 'indecent exposure'. This is for instance the case in Argentina (Article 129 Argentinian Penal Code).
[39] See section 474.27A of the *Criminal Code Act 1995* (Cth).

with minors in national law. In table 3 below we summarise how each of the jurisdictions under examination have criminalised webcam sex tourism.

While webcam sex has been criminalised in different ways throughout the countries presented in this report, some possibly complicating issues exist regarding the criminalisation *per se* or the harmonisation of criminalisation at the international level. Below we will briefly discuss these.

3.3.1 Definition of a child/ minor

When it comes to the criminalisation of webcam sex with minors (or any other form of sexual activity with minors for that matter), there is no full harmonisation on the age below which engaging in sexual activities with a person is deemed illegal. While on the supranational level there is general consensus as to the definition of a child (or minor), there is no full harmonisation on age in crime descriptions at the national level.[40]

In the CRC, a child (minor) is defined in article 1 as:

> *(...) a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.*

This definition applies to the Convention itself and to the OPSC.[41]

Article 3(a) of the Lanzarote Convention defines a child (minor) as:

> *(...) any person under the age of 18 years.*

The negotiators of the Lanzarote Convention considered the possibility of harmonising criminal law in the area of child exploitation by establishing the age of sexual consent in the Convention, but it was ultimately decided to let the member States decide for themselves at what age sexual activities with a person are deemed legal. The main reason for this being that this age varies greatly in Member States of the Council of Europe because of cultural differences.[42]

Nevertheless, for most jurisdictions under investigation in this report, a minor means a person below the age of 18 years and in most cases sexual activities involving such a minor are prohibited, unless explicitly stated otherwise. Some divergences can exist regarding the age of valid consent to sexual activities.

When it comes to sexual activities involving Sweetie, it is also relevant to take into account that Sweetie depicts a person that is under the age of twelve. At this age, there will be no discussion in the jurisdictions under investigation that Sweetie is a minor and that any form of

[40] See also: Interagency Working Group on the Sexual Exploitation of Children 2016, *Terminology guidelines for the protection of children from sexual exploitation and sexual abuse*, Luxembourg.
[41] The OPSC refers in the preamble to Article 1 of the CRC.
[42] *Explanatory report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. CETS 201*.

sexual activity involving a 12-year old is prohibited. Moreover, for many countries engaging in sexual activities with a minor the age of Sweetie is an aggravating circumstance (e.g. Argentina, the USA, Spain and Canada).

3.3.2 Relevance of physical presence

Given that webcam sex is a relatively new phenomenon, substantive criminal laws in many countries have not been amended to specifically include webcam sex as an offence in itself. In most cases, existing crime descriptions cover webcam sex. Most of these descriptions however stem from a time when engaging in sexual activities with a minor required physical contact with the victim. This raises the question whether the physical element in the crime descriptions is of material importance, or whether these crime descriptions also cover sexual activities taking place via a webcam, without out any physical contact or physical presence.

In several of the countries under investigation webcam sex with minors is considered sexual abuse. In the Netherlands, for instance, the Dutch Supreme Court decided that for sexual assault (article 247 of the Dutch Criminal Code) physical contact between the assailant and the victim is not necessary.[43] This means that when the perpetrator is participating in a webcam session with a person under the age of 16 and the victim performs sexual acts (such as performing sexual acts with themselves or a third person), the perpetrator can be held accountable for sexual assault. In Canada, webcam sex may be considered sexual abuse if the perpetrator invites the victim to touch him or herself (Section 152 Canadian Criminal Code). Furthermore, physical presence is also not a requirement for the offence of indecent exposure. The court held that the element 'in any place' could also refer to the Internet.[44] In Belgium, the adult who induces or forces a minor to display breasts or genitals or to perform sexual activities in front of the webcam is committing the offence of indecent assault (article 372 or 373 of the Belgian Criminal Code). In Turkey, however, physical contact is still considered an integral part of the offence of sexual abuse, which means that the sexual abuse of minors via the Internet could never fall within the scope of article 103 of the Turkish Criminal Code.[45]

Apart from offences that fall into the category of sexual abuse, the Lanzarote convention also opens up the possibility to criminalise pornographic performances viewed via a webcam:

> *'Article 21 incriminates certain conducts relating to the participation of children in pornographic performances. Paragraph 1 a and b are elements relating to the organisation of pornographic performances involving children while c relates to the spectator. As with child prostitution and child pornography, the provision establishes links between the supply and the demand by attaching criminal liability to the organiser of such pornographic performances as well as the customer. Depending on States, this provision may also cover the situation of persons who are*

[43] See: ECLI:NL:HR:2004:AQ0950.
[44] R v Alicandro [2009] ONCA 133 (CanLII).
[45] See Önok, M and Bayamlıoğlu, E, *Substantive and procedural legislation in Turkey to combat webcam-related child sexual abuse* (Turkey report), section 2.2.3, p. 16.

spectators of pornographic performances involving the participation of children through such means of communication as webcams. '[46]

From the above we may conclude that while the element of physical presence does not necessarily preclude the application of existing crime descriptions such as those covering sexual abuse. However, this must be decided on a country-by-country basis.

3.3.3 Substantive criminal law legality principle

A third issue related to the criminalisation of webcam sex tourism is that of substantive criminal law legality (*nulla poena sine lege*). As described above, substantive criminal laws in many countries have not been amended to specifically include webcam sex as an offence in itself. Rather, webcam sex is 'read' into existing crime descriptions. As such, one could argue that the crime descriptions lack the requisite legal clarity and certainty (*lex certa*) to be applied to online contexts. Based on the examined case law for the different countries, we have no indication though that this is indeed the case.

3.3.4 Differences in approach to the criminalisation of webcam sex

Based on the criminal law systems of the countries under investigation, we may conclude that webcam sex with minors is generally considered criminal in one way or another. In most countries webcam sex with minors falls under the heading of offences related to child pornography. Depending on the country and the circumstances of the case, webcam sex with minors may also fall under different crime descriptions such as sexual abuse or child prostitution, offences that generally carry higher penalties. This is, however, very much dependent on the circumstances of the case and the specific jurisdiction.

While there are differences in the approach to the criminalisation of webcam sex, they do not seem very problematic in the global fight against webcam child sex tourism. All of the jurisdictions examined have a more or less complete inventory of possible offences that apply in the context of webcam sex with minors.

An issue that needs to be taken into account though is that of double criminality.[47] Given the different approaches to the criminalisation of webcam sex, combating webcam sex tourism in an international context is more difficult. For instance, in the Netherlands webcam sex with a minor may qualify as 'sexual abuse', whereas in Turkey it only qualifies as 'sexual harassment' given that physical contact is necessary to proof sexual abuse. As such, law enforcement will need to assess whether the crime descriptions are sufficiently similar as not to cause issues of (a lack of) double criminality.

[46] *Explanatory report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. CETS 201*.

[47] The principle of double criminality was introduced by extradition treaties and requires the act to which a request relates to be a crime under both the criminal law of the requested state and the requesting state. For a comprehensive discussion on this see Williams, SA 1991, 'The Double Criminality Rule and Extradition: A Comparative Analysis', *Nova L. Rev.*, *15*, p. 582.

The table below shows which criminal provisions potentially apply to webcam sex in the countries under investigation. The table fields marked in red indicate that the existing country legislation is not applicable in the context of webcam child sex tourism.[48]

Table 3: Legislation applicable to webcam child sex tourism						
	18. Sexual abuse	19. child prostitution	20. child pornography	21. pornographic performances	22. corruption of children	23. Online solicitation (grooming)
Argentina			128 CC	128 CC	128 CC	131 CC
Australia	272.11 Criminal Code Act 1995 (CCA)	-[49]	474.19 CCA 474.20 CCA	272.14 CCA	272.9 CCA 474.27 A	272.15 CCA
Belgium	372 Belgian Criminal Code (BCC) 373, 375 BCC	379, 380 BCC 372, 373 and 375 BCC	383 *bis* BCC 371/1 BCC	379 BCC 380 BCC	385 BCC	377*quater* BCC 433bis/1 BCC
Brazil	217-A Brazilian Criminal Code (CPB) 241-D Children and Adolescent Statute (ECA) 213 ECA	218-B CPB	218-B CPB	217-A CPB 241-D ECA 241-E ECA	218 CPB	218B CPB
Canada	152 Canadian Criminal Code (CCC)	286.1 (2) CCC. 286.3 (2) CCC	163.1 CCC	163.1 CCC	173 (2) CCC	170 CCC 172.2 CCC 172.1 CCC
Croatia	158 Croatian Criminal Code (CrCC) (159 CrCC)	162 CrCC	163 CrCC	164 CrCC 165 CrCC	160 (1) CrCC	161 CrCC
England and Wales	8, 10, 17, SOA 2003	47, 48, 50 SOA	7(7), Protection of Children Act 1978 (?)	12 SOA 2003 or OPA 1959	12 SOA	14, 15 SOA
Estonia		175 (1) EPC[50]	175[1] EPC	175[1] EPC	179 EPC	178[1] EPC

[48] These provisions focus mostly on the actual physical contact between victim and offender, and are thus classical 'offline' offences.

[49] The term 'child prostitution' and the corresponding offence is more explicitly regulated under State/ Territory laws. However, there is no case law applying this kind of offence to the online context, and the jurisdictional reach of such State/ Territorial laws is more limited.

[50] 175(1) EPC refers to the '*influencing* of a person of less than eighteen years of age in order to cause him or her to commence or continue the commission of a criminal offence, begging, engagement in prostitution […]'. Usually, the provision would be an 'offline' offence. Yet, since it is possible that *influencing* is achieved through

			178 EPC	178 EPC		
Germany	176 (4) no. 1 StGB; 176 (4) no. 2 StGB	176 (4) no. 2 StGB	176a (3) in conjunction with §184b StGB	176 (4) no. 2 StGB	176 (4) no. 4 StGB	176 (4) no. 3 StGB
Israel	345–351, 203B Israeli Penal Code	203B IPC	214B (3) IPC	214B (3) IPC	208 IPC	203B IPC
Netherlands	247 Dutch Criminal Code (DCC) 246 DCC 248a DCC	246b DCC 248f DCC 250 DCC	240b DCC		240a DCC, 248d DCC	248e DCC
Nigeria	32 (1) Child Rights Act (CRA)	222A Nigerian Penal Code (NPC) 223 (2) NPC 2234 (4) NPC	281 NPC, 30 (2) (e) CRA 23 (1), (3) (c) Nigerian Cybercrimes Act (NCA)	30 (2) CRA	23 (3) a NCA	23 (3) a NCA
Philippines	2(h) Rules and Regulations on the Reporting and Investigation of Child Abuse Cases	3 (h) Anti-Trafficking in Persons Act of 2003 (ATPA)	3(a),(b). Anti-Child Pornography Act of 2009 (ACPA) 3(h), (j) ATPA 4 (c) 2 Cybercrime Prevention Act of 2012 (CPA)	9 Special Protection of Children Against Abuse, Exploitation and Discrimination Act 16-18 Revised Penal Code (RPC)	340 RPC	3(h),(i) ACPA
Poland	204(4) Polish Criminal Code (PCC)	199 (3), 200 (1), 203, 204 PCC	202 §3, 4, 4a, 4b, 4c PCC	Article 200a PCC	Article 200 §3, 4, 5 PCC	Article 200a PCC
Scotland	-[51]	9 Protection of Children and Prevention of Sexual Offences Act 2005 (PCPSO)	-	-	23, 24, 25, 33, 34, 35 Section 23 Sexual Offences Act 2009	1 PCPSO
South Korea		Articles 12 (2), 13 (2) of the Act on the Protection of Juveniles	Article 44-7(1)1 of the Act on Information Promotion and Protection, and Communications	Articles 287 and 294 of CA	Article 13 (2) of the Act on Special Cases concerning the Punishment, ETC. of	Articles 12 (2), 13 (2) of the Act on the Protection of Juveniles

online means only, the norm should be applicable in the context of webcam child sex tourism as well. However, at the moment of writing of this report there is no case-law to confirm this interpretation.

[51] Incomplete information based on country report.

		against Sexual Abuse	Network Utilization		Sexual Crimes; Articles 287 and 294 of CA	against Sexual Abuse
Spain	183 bis, 171, 172,183 Spanish Criminal Code (SCC)	Art. 189 SCC	Article 183 bis, 189.4. 189.5. 189.6, 189.7 SCC	Article 183 bis, 189.4. 189.5. 189.6, 189.7 SCC	Articles 183 bis, 185, 186 SCC	Article 183 ter, section 1 section 2 SCC
Turkey	105 Turkish Penal Code (TPC) – (only harassment)	227 TPC and possibly 80 TPC	226 TPC	226 TPC	226, 105 TPC	
United States			18 U.S.C. § 2252 18 U.S.C. § 2252A 18 U.S.C. § 1466A	18 U.S.C. § 2251	18 U.S.C. § 1470	18 U.S.C. § 2422(b)

3.4 Complicating factors in substantive law related to Sweetie

In this section, the two problematic issues will be addressed when it comes to applying existing substantive criminal laws to cases involving Sweetie. First, Sweetie is an avatar, a virtual character, programmed to appear and talk as a child but clearly no real child is ever involved in the process. Second, the avatar does not undress and therefore no sexually explicit behaviour on the part of the 'victim' takes place. This section investigates to what extent interaction with Sweetie is still deemed criminal despite the lack of involvement of both a minor and explicit sexual behaviour.

3.4.1 Virtual 'victim'

Sweetie's most important asset from an ethical perspective – the fact that it does not involve real children and thus does not put actual children at risk – at the same time may be problematic with regard to some (or most) of the criminal systems at hand and the application of their provisions as discussed previously. The reason for this is that the crime descriptions in most criminal law systems deal with real victims as opposed to 'virtual' victims.

Criminal law protects society (in this case minors) against harm through threat of sanctions (general prevention). Most of the crime descriptions in criminal law therefore criminalise specific behaviour, which in most cases constitutes a direct threat to something or someone. For example, in the case of murder or homicide, human life is threatened. In the case of theft, personal property is at risk. Thus, most crime descriptions feature the main elements of the situations they aim to address, often in relation to the persons they aim to protect. Generally, if the completed act does not match a crime description, then that particular crime cannot be proven. Most of the crime descriptions examined in this research - virtual child pornography and grooming being notable exceptions - feature real persons (minors), given that they are the objects of protection. This means that without a real victim, there is no crime. Since Sweetie is an AI system and hence does not qualify as a natural person, interaction with Sweetie will most likely not fulfil most of the crime descriptions discussed previously. An interesting exception, however, is the Philippines, where 'any lascivious exhibition of sexual organs or sexual activity

[…] with the aid of a computer system' is a punishable offence. This does not require an actual victim at all, and the law can thus be applied to interactions with Sweetie where the perpetrator displays his sexual organs before the webcam.

In the laws governing the sexual exploitation of minors, two types of criminal acts exist that do not focus on actual victims, but rather on the behaviour of the suspect and the intent that the particular behaviour signals. These crimes are: 1) virtual child pornography and 2) grooming.

Ad 1) Virtual child pornography
As described in section 3.2.2.3, not only real but also virtual child pornography is considered criminal, including computer-generated images not involving real victims. There are several reasons why criminal liability is also extended to virtual child pornography. These include avoiding evidentiary problems and the fact that the materials can be used to corrupt children, as well as the idea that virtual child pornography may act as a 'stepping stone' for consumers of child pornography, prompting them to move to real child pornography or possibly even sexual abuse.

Ad 2) Grooming
Grooming is the act of having contact with a minor for the purpose of arranging a meeting with this minor in order to engage in sexual activities or other lascivious conduct or to create child pornography. As it provides such a clear and present danger to the well-being of minors, in most of the jurisdictions under discussion grooming is a crime in itself, regardless of whether the meeting actually takes place or leads to sexual abuse. The process of grooming typically starts with rather innocent chats and develops through time into interactions which separately may constitute, among others, indecent communication, corruption of children, sextortion et cetera.

In some jurisdictions, it is not even necessary that a real minor is groomed. In these jurisdictions, law enforcement's imperative to employ investigative powers (e.g. luring suspects) has prompted changes to substantive criminal law. The investigative method of using a lure that is ostensibly a child would not be possible without the element in the crime description allowing for adults or virtual minors to be the object of the offence. In England and Wales for instance, the fact that the offender's communications are transmitted to a virtual child is unproblematic in regard to section 14, SOA 2003. The section's purposely wide language does not require the involvement of a child, but focuses rather on intent or belief on the part of the suspect that a child sex offence will take place.[52] The same goes for Australia where for instance section 474.28 (9) of the Criminal Code Act 1995 covers virtual children with the term 'fictitious recipients'. Noteworthy is also the Belgian offence of cyber-luring which codifies a similar rationale – according to the provision someone completes the criminal act upon communication with an apparent or probable minor.[53] Finally, the Philippine law on cybersex, while not specifically focused on grooming, declares *'any lascivious exhibition of*

[52] See Gillespie, AA, *Substantive and procedural legislation in England & Wales to combat webcam-related child sexual abuse* (report on England and Wales), p. 29.
[53] Cyber luring is codified in Art. 344bis/1 of the Belgian Criminal Code. See Royer, S, Marlier, G and Conings, C, *Substantive and procedural legislation in Belgium to combat webcam-related child sexual abuse* (Belgian report), p. 21.

sexual organs or sexual activity […] with the aid of a computer system'[54] a punishable offence *per se* and does not require an actual victim at all. At the time of writing this report, changes to Dutch criminal law are pending that would also include communicating with adult persons in the grooming crime description, but not communicating with virtual minors.[55]

From these two crimes we may deduce that in the area of protection against child exploitation substantive criminal law is not only reactive in nature and focussed on actual victims, but also preventative in the sense that it criminalises behaviour (regardless whether said behaviour is aimed at an actual minor) that may provide future danger to minors, or an indication thereof.

Apart from these two offences though, directly applying substantive criminal law provisions to virtual characters is still an untested area in most of the jurisdictions investigated for the present project. This is true for instance for both the Nigerian[56] and the Scottish criminal law.[57] In Canada the issue has been litigated in relation to some of the offences with the result of conviction of an offender who thought to be communicating with a child that never existed;[58] however, this approach is complemented by the law of attempts.[59] Criminal liability through attempt also seems to be the only avenue for criminalising a sexually-charged interaction with Sweetie in Argentina, Croatia, Estonia, Israel, Poland and Turkey. Construing an attempted offence is further possible regarding all other relevant provisions of the countries discussed above and will be addressed in the section on criminalisation of attempt under section 3.5.

3.4.2 No sexually explicit behaviour or nudity on the part of Sweetie

A second complication is that Sweetie is not programmed to undress or display sexually explicit behaviour. This means that (the animations of) Sweetie cannot be qualified as child pornography given that Sweetie does not engage or seemingly engage in sexual activities or show genitalia primarily for sexual purposes.

As a result, someone interacting with Sweetie cannot complete the offence of accessing (and possibly storing) child pornography. From a law enforcement perspective this is an issue, given that in most countries accessing (virtual) child pornography would be the go-to offence in the case of Sweetie.[60]

While an attempt at accessing (virtual) child pornography might still be construed, it usually carries a lower maximum penalty, and in some jurisdictions might not be an offence at all.

---

[54] Cybercrime Prevention Act of 2012, sec 4(c)(1).
[55] Schermer, BW, Koops, BJ and Van Der Hof, S, *Substantive and procedural legislation in the Netherlands to combat webcam-related child sexual abuse* (Dutch report), p. 17.
[56] See Orji, UJ, *Substantive and procedural legislation in Nigeria to combat webcam-related child sexual abuse* (Nigerian report), section 2.3.
[57] See Richardson, A, Kerr, M and Keane, E, *Substantive and procedural legislation in Scotland to combat webcam-related child sexual abuse* (Scottish report), p. 16.
[58] See Hodge, R, Substantive and procedural legislation in Canada to combat webcam-related child sexual abuse (Canadian report), p. 28.
[59] See s24 of the Canadian Criminal Code, RSC 1985, c C-46.
[60] Many of the other offences concerning webcam sex with minors would require additional acts on the part of the perpetrators, such as exposing themselves.

3.5 Criminalisation of attempt

The two complicating factors of Sweetie (it being a virtual victim and the absence of sexually explicit behaviour or nudity) have the effect that in most jurisdictions many of the criminal offences discussed in section 3.2.2 cannot be committed. But while a completed offence may be unable to be proven, an attempt might be.

For a completed criminal act, the offender must have fulfilled all components of the respective crime description, which – put in a nutshell – refer to the objective elements (a certain act or omission directed against a legally protected right, which has produced a certain result), and the subjective elements (concerning the offender's internal characteristics, in particular the intent to commit the act in question). Attempted crimes, in contrast, are prosecuted when the suspect has started to execute the crime he/she intended to commit, but failed to complete the criminal act due to external circumstances. In general, the rationale behind the criminalisation of an attempt lies with the dangerousness of the offender, who has failed to complete the intended crime at the given moment, but who has nevertheless clearly manifested activities that can easily result in a completed crime on the next occasion.

It is clear that only a handful of offences could be directly applied to virtual victims like Sweetie. Most of the provisions' descriptions require the offender's interaction with a *real* person, whose rights and interests must be at stake. Evidently, Sweetie is a computer-generated character, which has no legal interests and therefore cannot fulfil said requirement. A completed offence against the avatar will therefore rarely be committed under the current legal framework. It is however worth exploring whether the missing piece of the puzzle – the crime's subject – can be found through the laws of attempt. Accordingly, the following subsections elaborate upon the difference between a completed criminal offence and an attempted one by outlining the requirements of attempt, and how these apply in Sweetie's case.

3.5.1 Qualification of an attempt

The laws governing attempt vary in the jurisdictions investigated in this study. Their differences manifest themselves mainly in the origin of the doctrine, the way in which it has been codified or in its legal consequences.[61] In general, all jurisdictions criminalise attempt and employ similar considerations in outlining its main requirements.

A criminal attempt is deemed to exist when the suspect executes an act towards the commission of the offence he/she intends to effectuate, said act is more than merely preparatory[62] and

[61] In the USA, for instance, there is no general crime of attempt in federal law. Instead, statutes include separate provisions regarding the criminalisation of the attempted crime, see Unikowski, J, *Substantive and procedural legislation in United States of America to combat webcam-related child sexual abuse* (US report), p. 12. In contrast, other jurisdiction like Argentina (Art. 42 of the Criminal Code), Australia (an attempt to commit a crime is a distinct offence in all Australian jurisdictions and the general doctrine is regulated by their statutes), Brazil (Art. 14 (2) CPB), England and Wales (s.1, *Criminal Attempts Act 1981*), Germany (§§ 22, 23 StGB), the Netherlands (Art. 45 DCC) and Poland (Art. 13 of the Criminal Code) have a general regime of attempt liability, whose provisions are then applied in conjunction with the ones of the respective offence. Yet other systems like Croatia, Belgium (articles 51-53 BCC), Nigeria (s. 4 of the Criminal Code; s. 27(1) (a) of the Cybercrimes Act) opt for both.

[62] Argentinian law requires a start of execution, see Art. 42 of the Criminal Code. The general trend in Australia also requires 'more than merely preparatory' acts, see Britten v Alpogut [1987] VR 929, at 938. The Polish

carried out according to the offender's intent.[63] Establishing the point at which mere preparation becomes a criminal attempt is a crucial part of the attempt liability, as it pinpoints both when a person becomes criminally liable and when authorities may intervene.[64] In practice, however, it may be challenging to demarcate the exact start of an attempt, but this concern is usually left to the courts to deal with and depends on the particular facts of the case and the available evidence.

Further, the laws of attempt differentiate between the reasons why the person failed to commit the crime. First, an attempt to commit a crime may fail either due to external circumstances, which are outside of the sphere of influence of the perpetrator.[65] Second, despite completing the intended actions the requirements set forth in the description of the crime might not be met. The latter is usually referred to as inadequate or inept attempt, and although recognized by all criminal systems in this study, it is applied in widely varying ways. These are of particular importance for prosecuting individuals interacting with Sweetie and will be addressed in the following subsections.

3.5.2 Inadequacy of an attempt

Because Sweetie is an avatar and, therefore, from a criminal law perspective an inadequate object in relation to sexual crimes, criminal liability for interacting with Sweetie needs to be examined through the lens of the doctrine of inadequate attempt. The doctrine of impossible or inadequate attempt takes account of situations, in which the completion of the intended offence is factually or legally impossible due to the object's unsuitability, the chosen time, or the means used by the perpetrator. We can distinguish between *relative* inadequacy of an attempt and *absolute* inadequacy of an attempt.

Relative inadequacy (factual impossibility)

Relative inadequacy occurs when an act does not bring about the results described in the crime description, because at the time of the attempt committing the crime was in fact impossible. In other words, circumstances outside the knowledge of the perpetrator make it impossible for the attempt to succeed. More specifically, relative inadequacy relates to the object of the crime and/or the means with which the crime is attempted.

Examples of an attempt that is relatively inadequate are trying to shoot a person with an unloaded gun (relative inadequacy of the means), or stealing money from an empty cash register (relative inadequacy of the object).

With a relatively inadequate attempt, the concrete facts of the case make it so that the attempt fails. If however the facts were as the perpetrator believed them to be, the attempt would have

criminal system requires speaks of a 'final and decisive action' towards the offence in question, see Polish report, p. 14.

[63] The Polish system refers to offender's 'decision', see p. 14 of the Polish report.

[64] Robinson, PH 2010, 'United States' in K Heller & M Dubber, (eds), *The handbook of comparative criminal law*, p. 579. The German attempt doctrine, for instance, has recognised several moments of commencing. The attempt can begin when one of the elements of the offence description is fulfilled, but also just before fulfilling any crime element as long as the offender undertakes steps which according to his plan are prior to the crime realisation and will immediately result in the completed offence. See Hakobyan, H, *Webcam Sex with (Virtual) Children: Legislative Gaps or Criminalised Conduct?* (German report), p. 65.

[65] In an online context, this would be the case if the offender's chat conversation with the victim is suddenly interrupted by a poor Internet connection or temporary unavailability of the server.

succeeded, as a result of which the perpetrator can be charged with a criminal attempt. The reasoning behind criminalising this form of attempt is nicely summarised in the US case of *State v. Moretti*:

> *When the consequences sought by a defendant are forbidden by the law as criminal, it is no defense that the defendant could not succeed in reaching his goal because of circumstances unknown to him.*[66]

Absolute inadequacy (legal impossibility)
Absolute inadequacy refers to those situations whereby an attempt can never lead to a completed offence, because what was attempted is not a criminal act (or in any case does not match with the relevant crime description). In the case of absolute inadequacy, the perpetrator intends to commit a crime but by virtue of the object or the means, the intended behaviour cannot result in a crime in reality. An example is trying to murder a corpse (inadequate object) or trying to poison somebody with very strong camomile tea (inadequate means). While criminal intent is present, the actual behaviour does not align with the crime description. Under the doctrine of absolute inadequacy, the suspect can never be held criminally liable, despite a clear display of criminal intent. The reasoning for this is that someone cannot be held criminally liable for something that is not criminal, even though that person might have thought that he or she actually was committing a crime.

Relative inadequacy is different from absolute inadequacy in that different facts could or would have made the attempt successful, while in the latter case the desired criminal outcome can never be achieved by the suspect.

3.5.3 Applying the law of attempts to Sweetie

The question is whether interacting with Sweetie would count as an attempt that is absolutely inadequate, or relatively inadequate. An answer to this question needs to take into account the circumstances of an actual case and the specifics of the doctrine of attempt in the national system. But having said that, we can make some general observations about applying the law of attempts to Sweetie.

It is not straightforward to determine whether Sweetie will lead to an absolutely inadequate attempt, or a relatively inadequate attempt. An argument in favour of an absolutely inadequate attempt is that Sweetie, being a virtual person, and programmed not to undress, is an absolutely inadequate object. The argument would then be that it is not criminal to engage in sexual activities with a virtual person, even if this virtual person is posing as a minor and the perpetrator thought that the avatar was a real person. But even if sexual activities with a virtual minor is criminalised in specific jurisdiction, than Sweetie might likely still be considered as absolutely inadequate given that she can never show sexual organs or perform sexual activities.

However, we can also take a somewhat broader perspective and qualify Sweetie as a relatively inadequate object for the crime of webcam sex with minors. The argument is than that the suspect wants to commit the crime of webcam sex with a minor and enters a chatroom with for

[66] State v Moretti, 244 A.2d 499.

instance twenty minors for this purpose. Unbeknownst to the suspect one of the twenty minors is Sweetie. The suspect is 'unlucky' and picks Sweetie. This case is comparable to the example of the cash register: under normal circumstance the crime would have been committed, but due to 'bad luck' on the part of the suspect, there is now a factual impossibility. If we are to follow this reasoning though, it must be clear from the behaviour of the suspect that had the suspect chosen a different child, the outcome of the behaviour would have been the same.

The attempt liability in the case of Sweetie would thus largely depend on whether the respective criminal system emphasizes the objective or subjective elements of the offence. Jurisdictions that focus on the objective elements underline the importance of the concrete crime object, while those systems that focus more on the subjective elements see the alleged offender and his mental state as a threat for the protected ideal good: minors and their overall safety and well-being. In these systems the intent of the suspect is crucial. The German law of attempts, as it will be explained below, is the only example where both objective and subjective considerations are decisive for the attempt liability of the offender.

In the following we illustrate which jurisdictions follow the first approach and which the latter.

The law of attempts in different jurisdictions

The country reports indicate that the doctrine's considerations would apply in cases where the victim of the intended crime is virtual, and thus a part of the crime description can never be fulfilled. Yet, while in some jurisdictions the suspect remains punishable or receives a lower sentence, in others the legal impossibility completely excludes criminal liability. Thus, depending on the particularities of the respective criminal system and on the circumstances of the case, a person may be found guilty of an *attempt* to commit webcam sex tourism notwithstanding the fact that he or she did not interact with a real minor, but with Sweetie.

Under Canadian, English, Israeli, Scottish and US[67] law, for instance, the reason why the offender's attempt failed is in most cases irrelevant,[68] as long as the perpetrator undertakes more than preparatory actions in pursuit of the prohibited behaviour and manifests malicious intent. In these jurisdictions the suspect's criminal intent (which has become apparent through his/ her actions) weighs more heavily than the objective fulfilment of the crime description.

England's criminal attempt law applies this premise to all offences related to webcam sex with minors save for s.127 of the Communications Act 2003,[69] while its Scottish counterpart does not foresee any limitations in application.[70] Canadian case law shows that Section 24 of the Canadian Criminal Code, which regulates attempt, is not always applied. However, this does

[67] In US law, the impossibility to victimise Sweetie is relevant as a defence that excludes punishability. Yet, such arguments of impossibility have not been successful in the prosecution of individuals attempting to commit a crime in cases where they believed that they were interacting with a child, but were in fact interacting with an undercover law enforcement officer. For more on the matter see the country report on the US, p. 12.

[68] See on the Australian doctrine Haughton v Smith [1975] AC 476, which was followed on the Scottish case law Docherty v Brown [1996] JC 48 at 50; See on the law of attempt in England and Wales *s.1, Criminal Attempt Act 1981*; see also s.24 (1) of the Canadian Criminal Code.

[69] The offence relates to the *sending* of an indecent or obscene message. It is irrelevant whether or by whom it is received, therefore the law of attempts is not required.

[70] See country report on Scotland, section 2.3, p. 17. However, covert operations where police Internet investigators have posed as children have not been challenged or judicially considered yet.

not have to do with normative restrictions on the application of the impossible attempts doctrine, but results from the fact that some offences carry included offences that are attempts.[71] Thereby, the law addresses the activities surrounding the core offence and circumvents possible loopholes. Accordingly, a conviction can be pursued for any of the webcam offences in relation to Sweetie and it will depend on the particular circumstances of the case whether the prosecution relies on s.24 or on the included offence. In Israel the law of impossible attempt can be applied to all criminal charges regardless of the reason of impossibility.[72] However, since the avatar does not undress, attempted aggravated indecency would be the most serious crime within the Israeli criminal framework.[73] In addition, both Israeli[74] and Canadian[75] law place the burden of proof upon the defendant when it comes to demonstrating that he was not aware of actually communicating with a minor. Under Australian law, in principle, the common law doctrine of attempts applies as well, and a suitable offence (under State/ Territory laws) might be an attempt to procure a child for a sexual act. However, it should be noted that many of the Commonwealth offences illustrated in the tables above are explicitly excluded from attempt liability.[76] The rationale behind the legislator's choice is the fact that many of the offences are already preparatory in nature, so that adding an attempt would over-extend criminal liability. Further, as indicated above, the preferred approach in Australia has been to explicitly allow for fictitious recipients of illegal communications, so that an attempt, although possible to construe in some if not in all cases, is not necessary for prosecution. Attempt liability in Germany[77] is regulated by § 22 StGB, while inadequate attempts are subject to the provision of § 23 (3) StGB[78]. According to the norm, when the suspect targets an inappropriate object, his liability depends on whether he evidently acted in 'gross ignorance'[79]. In case the gross ignorance was evident to a reasonably informed person the court may mitigate the sentence or entirely leave out the punishment. Otherwise a punishable inadequate attempt is given.

Applying the doctrine outlined above to the case at hand means the offender would be liable for attempted sexual abuse pursuant to § 176 StGB, if Sweetie looks like a real child to every informed person. Thus, even though the avatar is an inadequate crime object because the chat interaction with the offender cannot be perceived by a real child, if the offender's sexual performance is transferred through a webcam to the chatbot, an attempted sexual child abuse in accordance with §176 (4) no. 1 in combination with §§ 22, 23 StGB would likely be given. The same applies to the provision of §176 (4) no. 2 StGB, when the offender tries to induce Sweetie to perform a sexual act. In such a scenario, the suspect's inducement would be

[71] For instance, the offence of obtaining sexual services from a minor includes also the offence of communicating with a person under 18 in order to obtain sexual services for consideration. See on that Canadian report, p. 29.
[72] The Israeli law of attempt is embedded in the Introductory Part of the Israeli Penal Code, Chapter 5, Article 1.
[73] See Harduf, A, *Substantive and procedural legislation in Israel to combat webcam-related child sexual abuse* (Israeli report), p. 11.
[74] See the Israeli Supreme Court decision in the case of *Ktiei v Israel,* LCrimA 1201/12 [9 January 2014].
[75] See for instance s. 171.1 (3) and s. 172.2(3) of the Criminal Code of Canada, RSC 1985, c C-46.
[76] See Australian report, p. 19.
[77] See the German report.
[78] 'Section 23 Liability for attempt. (…) 3) If the offender due to gross ignorance fails to realise that the attempt could under no circumstances have led to the completion of the offence due to the nature of its object or the means by which it was to be committed, the court may order a discharge, or mitigate the sentence as it sees fit (section 49(2)).'
[79] Gross ignorance ('*grober Unverstand'*) is given when the suspect does not realise that under no circumstances his acts could complete the offence.

completed and would amount to an attempt, once the offender is convinced that he has done everything necessary to influence a child and the latter is just about to start performing.[80]

In Poland, the law of impossible attempts in Article 13 (2) of the Criminal Code would allow construing a punishable attempt for the offences outlined in Art. 202a (1 and 2) and Art. 200 (4) of the Criminal Code, i.e. the solicitation of minors for sexual purposes and corruption of minors respectively.[81]

The Estonian legislation (section 26 of the Penal Code) and case law suggest that an impossible attempt regarding a webcam interaction with Sweetie is also likely to be punishable, especially in relation to the offences of sexual enticement of a child and agreement to meet a child for sexual purposes.[82]

In Nigeria, a person who is approaching Sweetie for webcam sex would be punishable for an attempt to indecently interact with a boy or a girl (sections 216 and 222 of the Nigerian Criminal Code respectively), and under section 23 (3) (a) of the Nigerian Cybercrimes Act. In relation to the latter, section 27 (1) (a) of the Cybercrimes Act clarifies that an attempted offence is punishable as a principal offence under the Act. The impossibility to commit webcam child abuse of a virtual minor is irrelevant pursuant to section 4 of the Nigerian Criminal Code.

The laws of attempt in Argentina, Belgium and Croatia are not as straightforward as the ones already discussed and therefore somewhat more challenging.

In general, the laws on attempt in Argentina are applicable to all types of crimes,[83] including all offences against sexual integrity. Art. 44 of the Argentine Criminal Code regulates the defence of impossibility, which reduces the sentence or even acquits the defendant when granted. It is in the light of this provision that courts consider (attempts to commit) impossible crimes. However, it appears that there are no clear criteria on how courts engage in an assessment of the action's efficacy in bringing about the intended crime.[84] Therefore, while the provision's rationale would apply to the case of Sweetie, it is unclear how and with what outcome.

In Belgium, the criminal liability for attempting a particular offence will depend on the offence itself.[85] The attempt to commit a crime is always punishable, while the attempt to commit a misdemeanour is punishable if the law explicitly provides it. In the case of Sweetie one of the potentially relevant offences is attempting indecent assault. However, a prosecution's outcome

[80] In the context of webcam child sex tourism, an indication for that could be that Sweetie agrees to perform and provides the means for the transfer of rewards (*e.g.* bank account number).
[81] See country report on Poland, p. 14.
[82] Kala, K, Substantive and procedural legislation in Estonia to combat webcam-related child sexual abuse (Estonian report), pp. 22-23.
[83] Ferrante, M 2010 'Argentina' in K Heller & M Dubber, (eds), p. 29.
[84] Ferrante, M 2010 'Argentina' in K Heller & M Dubber, (eds), p. 31.
[85] Attempts to possess or access virtual child pornography are not punishable, see Art. 383bis BCC. The same applies to the attempt to commit the offence of publicly outraging morality by actions who offend modesty, Art. 385 BCC. See for more on the matter Belgian report, p. 22.

will very much depend on the court's approach towards impossible attempts. If the protected object (here minors, who are not at risk through the act since Sweetie is not a minor) is deemed more relevant than the subjective state of mind of the offender, acts involving Sweetie will not be punishable.[86] Furthermore, an attempt to access (virtual) child pornography is also not punishable in Belgium.

The Croatian law of attempts in its turn does not substantively differ from the already discussed doctrines.[87] Inadequate attempts are punishable as ordinary ones, but here it is the interpretation of the attempts provision that turns out to be problematic. A perpetrator attempting to commit an offence by inappropriate means or against an inappropriate subject may be exempted from liability due to 'rough irrationality'[88]. However, Croatian law does not provide a definition of 'rough irrationality' and courts have not dealt with the term either. Whether an offender is exempted from punishment in each case of rough irrationality, or only when his/ her criminal intent results from the rough irrationality, remains unclear. To what extent impossible attempts have an impact on cases involving Sweetie is still to be determined.

A final remark concerns impossible attempts under Dutch, Spanish and Turkish criminal law. Dutch (case) law distinguishes between relatively inadequate and absolutely inadequate attempts. An attempt to have webcam sex with Sweetie would most likely constitute an absolutely inadequate attempt, which is not punishable regardless of the criminal intent of the alleged perpetrator.[89] A possibility to use Sweetie under current Dutch criminal law might be found in the article on child pornography (240b Sr). As indicated previously,[90] the crime of child pornography does not require that a person below the age of 18 is pictured. The inclusion of 'seemingly involved' in the provision means that virtual child pornography is punishable as well. The addition of the text 'seemingly involved' negates the issue that Sweetie is considered an absolute inadequate object given the fact she is not a real girl. As such, trying to get access via webcam to child pornography, or trying to produce and possess child pornography by recording and storing the webcam stream, even if involving an avatar, could be construed as a criminal attempt at accessing (or producing or possessing) child pornography. While this negates the issue of the virtual nature of Sweetie, it does not necessarily mean Sweetie is then an adequate object. Given that Sweetie will never portray sexual behaviour or any nudity for that matter, as it is not part of her programmed features, she might still qualify as absolutely inadequate on those grounds. If Sweetie were programmed to show sexual behaviour or sexual organs this would make proving the suspects' intent to have criminal webcam sex more straightforward, but this is not the case at present.

[86] See Belgian report, p. 22.
[87] See Bojić, I, *Substantive and procedural legislation in the Republic of Croatia to combat webcam-related child sexual abuse* (Croatian report), p. 20.
[88] The respective provision reads: 'The perpetrator who attempts to commit a criminal offense by inappropriate means or against an inappropriate object, *due to the rough irrationality,* may be exempted from punishment.' See Croatian report, p. 20.
[89] See Dutch report, pp. 5 and 16.
[90] See section 3.2.1 Virtual 'victim' of this report.

The Spanish criminal system in general does not punish impossible attempts.[91] However, recent case law has opened up the possibility for punishing impossible attempts by stipulating that impossible attempts should be punished when an *ex ante* evaluation of the suspect's conduct leads a reasonable person to believe that the consummation of the offense was possible even though an *ex post* study of the facts reveals that it was impossible for the actor to consummate the offense.[92] Consequently it could be argued that if a reasonable person sees Sweetie in the webcam stream and believes it to be a real ten-year old, an attempt would still be construed even if in the aftermath it is revealed to the person that the child he/ she saw was a computer-generated fiction. It remains to be seen how this approach will be implemented in prosecuting suspects of online sex crimes involving an inadequate object, such as Sweetie.

In Turkey, impossible attempts are recognised as a legal construct, the consequences of which are unclear. Some argue that impossible attempts should be punishable, but others do not agree. So far, the courts have not settled the dispute,[93] as a result of which it is unclear whether an interaction with Sweetie might amount to an attempted sexual harassment pursuant to Art. 105 of the Turkish Criminal Code.

The table below gives an overview of the possibilities for criminalising (attempted) webcam sex with Sweetie. The fields marked in green refer to provisions which can be applied without further ado, while those in orange relate to provisions whose use in the context at hand has not been confirmed in case law yet. Red indicates that no provision applies.

Table 4: Criminalisation of (attempted) webcam sex with Sweetie

	18. Sexual abuse	19. child prostitution	20. child pornography	21. pornographic performances	22. corruption of children	23. Online solicitation (grooming)
Argentina	Possibly attempt	Possibly attempt	Possibly attempt	Possibly attempt	Possibly attempt	131 ACC
Australia	272.11 Criminal Code Act 1995 (CCA) (attempt)		474.19 CCA 474.20 CCA		474.27A	474.28(9) CCA
Belgium						433 bis 1 BCC Art. 143 §3bis Act Regarding Electronic Communication
Brazil						

[91] See Agustina, JR and Valverde, R, *Substantive and procedural legislation Spain to combat webcam-related child sexual abuse* (Spanish report), p. 14. For more on the matter see also Gómez-Jara, C and Chiesa, LE 2010 'Spain' in K Heller & M Dubber, (eds), p. 503.
[92] Gómez-Jara, C and Chiesa, LE 2010 'Spain' in K Heller & M Dubber, (eds), p. 503. SSCS February 16, 2007, available from: www.westlaw.es, Ref: RJ 2007\2381.
[93] See country report on Turkey, section 2.2.3, p. 18.

Canada	152 CCC (attempt)	286.12 CCC (attempt) 286.32 CCC (attempt)	163.1 CCC (attempt)			
Croatia	Possibly attempt	Possibly attempt	163 CrCC	Possibly attempt	Possibly attempt	Possibly attempt
England and Wales	8, 10, 17, SOA 2003 (attempt)	47, 48, 50 SOA (attempt)	7(7), Protection of Children Act 1978 (possibly attempt)		12 SOA (attempt)	14, 15 SOA (attempt)
Estonia	Possibly attempt	Possibly attempt	178 EPC	Possibly attempt	179 EPC	178[1]EPC
Germany	Possibly attempt	Possibly attempt	Possibly an attempt of 184b (3) StGB		Possibly attempt	Possibly attempt
Israel	Possibly attempt	Possibly attempt	Possibly attempt	Possibly attempt	Possibly attempt	Possibly attempt
Netherlands						
Nigeria	216, 222 NCC	222NCC		23(3) (c) NCA jo 27(1) NCA (attempt)	23(3)(c) jo 27(1) NCA (attempt)	23(3)a jo 27(1) NCA(attempt)
Philippines					Possible attempt at cybersex (showing genitalia)	3(h), 3(i) Possibly attempt
Poland	204 (4) Polish Criminal Code (PCC), possibly attempt	199 (3), 200 (1), 203, 204 PCC, possibly attempt	202 §3, 4, 4a, 4b, 4c PCC. Possibly attempt	200a PCC. Possibly attempt	200 §3, 4, 5 PCC. Possibly attempt	200a PCC. Possibly attempt
Scotland		9 PCPSO (attempt)			23, 24, 25, 33, 34, 35 Section 23 Sexual Offences Act 2009 (attempt)	1, 9 PCPSO (attempt)
South Korea		12 (2), 13 (2) APJSA (possibly attempt)	44-7(1)1 of the Act on Information Promotion and Protection, and Communications Network Utilization (possibly attempt)	287 and 294 of CA (possibly attempt)	13 (2) of the Act on Special Cases concerning the Punishment, ETC. of Sexual Crimes (attempt); 287 and 294 of CA (possibly attempt)	12 (2), 13 (2) APJSA (possibly attempt)

Spain			Article 183 bis, 189.4, 189.5, 189.6, 189.7 SCC (attempt)			
Turkey	105 Turkish Penal Code (TPC), possibly attempt	227, 80 TPC, possibly attempt	226 TPC, possibly attempt	226 TPC, possibly attempt	226 TPC, possibly attempt	
United States			18 U.S.C. § 2252, 2252A, § 1466A (possibly attempts)	18 U.S.C. § 2251 (possibly attempt)	18 U.S.C. § 1470 (possibly attempt)	18 U.S.C. § 2422(b) (attempt)

3.6 Summary and conclusion

Most of the criminal systems discussed in the previous sections seem well-equipped to combat webcam sexual crimes against *real* minors. Some have introduced new legislation to specifically tackle these types of online crimes, while others do not distinguish between online and real world offences, and thus do not encounter systematic difficulties in applying the criminal norms to the cyber environment.

However, we do see a divergence in how webcam sex is criminalised. As will be shown in the following chapters, this finding impacts the possibilities for cross-border law enforcement, and often impacts the outcome of transnational investigation procedures.

In some countries, webcam child sex tourism is considered sexual abuse or sexual harassment, while in others it is a form of child pornography but does not fall under the heading of sexual abuse. Generally speaking though, most countries under examination have a full inventory of crimes that can apply to webcam sex tourism. What is relevant to consider in this context is that different types of interactions between victim and perpetrator may trigger different articles under (domestic) criminal law. For instance, merely talking to a minor without sexual content or hinting at sexual activities[94], does not yet trigger any criminal law provisions, but sending indecent pictures or promoting sexual activities falls under the heading of corruption of a minor and possibly even grooming. When the victim is engaged in sexual activities and/or genitalia are exposed via webcam, this may trigger offences such as child pornography and pornographic performances, and possibly sexual assault. If payment is involved, provisions regarding child prostitution come into play. Finally, if the perpetrator exposes him/herself and masturbates or forces or coerces the victim to do or undergo sexual activities, this may constitute corruption of minors or even sexual assault.

[94] Please note that a sexualised conversation could be for instance an offence in England and Wales under the Communications Act 2003. Further, a typed conversation could amount to an offence under the Obscene Publications Act 1959. Also, when s.15A, Sexual Offences Act 2003 comes into force it would be illegal under that provision.

While all countries under investigation have criminalised webcam sex in one way or another, the situation is less clear-cut when Sweetie, a chatbot rather than a person, is involved in the interactions. In a few countries webcam sex with a virtual person is criminalised (see Table 5 below). In these countries, the criminal law provisions focus on the behaviour and the intent thereof, rather than on the behaviour in relation to the result it brought about.

In those countries where the crime descriptions only mention real minors as the object of protection, interaction with Sweetie may still qualify as an attempt at illegal webcam sex. In this area we see a further divergence. In some countries an attempt at webcam sex with Sweetie can be construed[95], in other countries an attempt at webcam sex with Sweetie is not deemed criminal because it qualifies as an impossible attempt. What is clear from our investigation that for most countries it still very much unclear whether prosecuting an attempt would be successful. It also relevant to note that an attempt generally carries a lower maximum penalty than a completed offence.

Finally, in those jurisdictions where neither a completed offence nor an attempt can be construed because of the virtual nature of Sweetie, interaction with Sweetie may still be qualified as an attempt to access to child pornography. However, in these countries we should also take into account the fact that an attempt may still be impossible given the fact that Sweetie will never show sexual organs or perform sexual acts. Furthermore, in some jurisdictions an attempt to access child pornography is not criminal in general.

[95] It must be noted though that in most of these countries the possibility of webcam sex with virtual minors has not been tested in court.

Table 5: Criminalisation of webcam sex			
	Webcam sex criminalised	Webcam sex with virtual person criminalised	Attempt at webcam sex with virtual person criminalised
Argentina	X	-	X (only likely for grooming)
Australia	X	X	X
Belgium	X	X (for the offence of cyber luring)	X (depending on the interpretation)
Brazil	X	-	-
Canada	X	X	X
Croatia	X	X	X (no case law yet)
England and Wales	X	-	X
Estonia	X	X (no case law yet)	X (no case law yet)
Germany	X	-	X
Israel	X	-	X
Netherlands	X	-	-
Nigeria	X	-	X
Philippines	X	-	X
Poland	X	-	X
Scotland	X	X (not tested yet)	X
South Korea	X	-	X (no case law yet)
Spain	X	-	X (child pornography only)
Turkey	X (only regarding sexual harassment)	-	X (possible, not tested yet)
USA	X	-	X

4 Criminal procedural law aspects

4.1 Introduction

Since Sweetie is intended as an investigative tool for law enforcement in online investigations, its implementation in law enforcement operations is governed by the laws of criminal procedure.[96] In this chapter we investigate what (online) investigatory powers are available in the jurisdictions involved in this study, and how these powers apply to Sweetie.

4.2 Human rights protection in (online) investigations

Human rights serve first and foremost as a control tool for modern state bureaucracy against structural injustices.[97] In this role, they perform a 'check and balance' function for states using coercive investigative powers. While international human rights law imposes on states the negative obligation to refrain from interfering with the exercise of human rights, this duty is balanced by the exigencies of everyday life and the positive state obligation to proactively protect the individual's rights from violations.[98]

In procedural criminal law, the interplay of these obligations is reflected in the enactment of special investigatory powers on the one hand (which temporarily limit the constitutionally guaranteed rights of the citizen in the fight against crime), and in the set-up of procedural rules that regulate, oversee and limit said special powers on the other. In either case, specific requirements must be met, some of which depend on the specific nature of the right itself, while others, as will be shown below, are of a more general nature.

It should be noted that in the European context, the ECtHR is particularly present in the human rights context and has assumed an active role in the interpretation of the ECHR. The Court's finding that both negative and positive human rights obligations stem from the ECHR in the context of law enforcement has been also widely followed and adopted by other human rights mechanisms, such as for instance the Human Rights Committee (HRC). The consideration of both positive and negative state obligations is thus a largely recognised tenet when it comes to the effective enforcement of individual rights.

In this research, we will focus specifically on the negative human rights obligations, and the extent to which states are permitted to infringe human rights for the purpose of combating webcam sex tourism.

4.2.1 Criminal procedure law requirements

Human rights have been decisive in shaping constitutional guarantees and hence have implications for the reach of state powers and the use of special investigative techniques. These

[96] Note that Sweetie may also be used as a deterrent. However, if Sweetie is used as a deterrent, it is likely only effective if there is a risk for the perpetrator that his behaviour may ultimately be exposed. In other words, if Sweetie is used as an investigative method.
[97] Bielefeldt, H 2012 'Philosophical and Historical Foundations of Human Rights' in C Krause & M Scheinin, (eds), *International Protection of Human Rights: A Textbook*, pp. 14-15.
[98] Bielefeldt, H 2012 'Philosophical and Historical Foundations of Human Rights' in C Krause & M Scheinin, (eds), *International Protection of Human Rights: A Textbook*, pp. 14-15.

powers have to abide by certain requirements to ensure the integrity of the criminal procedure and the reliability of the obtained evidence. In addition, special investigative powers often have to remain the exception to the rule.[99] Consequently, state agencies may interfere with the individuals' rights only in exceptional circumstances and pursuant to the requirements of proportionality and subsidiarity. Furthermore, the use of intrusive state methods is only allowed if they are in accordance with the legality principle, in other words, if they have a specific legal basis in the law of criminal procedure.

The European Convention on Human Rights (ECHR), more specifically 8 ECHR, gives a good overview of the elements needed when doing the balancing test between law enforcement requirements and human rights. We will therefore use it as our point of departure for the discussion on criminal procude law aspects. The elements the ECHR stipulates are the following:

Necessity
Necessity refers to the test of 'necessary in a democratic society'. The latter implies in its core a finding of proportionality,[100] while at the same time considering the particular circumstances of the case, including 'the nature, scope and duration of the measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them and the kind of remedy provided by the national law'.[101] The proportionality test ensures that investigative tools and methods impair the legitimate interests of the alleged offender in a way that is reasonably proportionate to the harm committed or threatened.[102]

Subsidiarity
The principle of subsidiarity requires law enforcement to employ a more intrusive means of investigation only where less intrusive solutions would be substantially less or not at all effective, and would thus jeopardise the aspired operation. We found that this tenet has been widely adopted by the investigated jurisdictions.

In accordance with the law (principle of legality)
Last but not least, criminal procedures can only take place, if and in a manner provided by the law. The rationale behind this principle of legality is strictly connected with legal certainty and aims to ensure that norms are available and accessible prior to the procedure that is being set in motion. Further, criminal procedures need to be foreseeable and predictable. This means that national laws need to be sufficiently clear as to under what circumstances law enforcement can make use of special investigatory methods. Individuals should also be able to determine which authority or mechanism implements and oversees the investigations.

[99] The country studies drafted for the purpose of this reports reveal that this is true for the majority of the civil law countries.
[100] *Klass and others v Germany*, Application no. 5029/7149, § 50; *Weber and Saravia v Germany*, Application no. 54934/00, § 116–118.
[101] *Weber and Saravia v Germany*, § 106.
[102] Ashworth, A and Horder, J 2013, *Principles of criminal law*, Oxford University Press, p. 56.

4.3 Use of investigative powers in an online context

In order to protect human rights and to safeguard the integrity of the criminal investigation, the principle of legality as described above stipulates that special investigative methods require a basis in the law. This has led to an inventory of special investigative powers codified in the laws of the jurisdictions under examination. Below (see table 6) we provide an overview which investigatory powers are available in the selected countries.

The specific investigative powers used in an online context are codified in the jurisdictions under examination more or less along the lines of those described in the Cybercrime Convention. Therefore, as it provides the most harmonised international framework governing the use of investigative powers, we use the Council of Europe Convention on Cybercrime as the framework for discussing investigative powers in an online context.

Given the close resemblance of Sweetie to the work of undercover agents, we will also discuss this investigative power, even though the Cybercrime Convention does not cover it.

Council of Europe Convention on Cybercrime
Article 16. Expedited preservation of stored computer data
Article 17. Expedited preservation and partial disclosure of traffic data
Article 18. Production order
Article 19. Search and seizure of stored computer data
Article 20. Real-time collection of traffic data
Article 21. Interception of content data
Other: *Undercover operations conducted on the internet.*

The countries examined in this report have codified the use of investigative powers in different ways.

Table 6: Codification of investigative powers in the selected jurisdictions							
	Preservation of stored computer data	Preservation of traffic data	Production orders	Search and seizure of stored computer data	Real-time collection of traffic data	Interception of content data	Undercover operations
Argentina	-	-	X	X	-	X	X
Australia	X	X	X	X	X	X	X
Belgium	X	X	X	X	X	X	X
Brazil	X	X	X	X	X	X	X[103]
Canada	X	X	X	X	X	X	X
Croatia	X	X	X	X	X	X	X
England and Wales	X	X	X	X	X	X	X
Estonia	X	X	X	X	X	X	X
Israel	-	-	X	X	X	X	-
Netherlands	X	X	X	X	X	X	X
Nigeria	X	X	X	X	X	X	-
Philippines	X	X	X	X	-	-	-
Poland	X	-	X	X	-	X	X
Scotland	/[104]	/	/	/	X	X	/
South Korea	-	-	-	X	-	-	-
Spain	X	X	X	X	X	X	X
Turkey	X	X	X	X	X	X	X
USA	X	X	X	X	X	X	X

The table above shows that the studied jurisdictions - with the exception of South Korea - have largely accommodated procedural provisions regarding undercover policing and online investigative techniques within their respective laws. In the following, we elaborate upon the necessary safeguards and admissibility conditions in relation to investigative powers in order to protect the rights and interests of individuals.

4.4 Sweetie as an investigative method

Before applying the procedural framework to Sweetie, we need to establish what kind of an investigative tool the avatar actually presents. We therefore first elaborate upon the nature of the chatbot/ avatar as an investigation tool and then establish whether and how its features fit the legal framework of criminal procedure described above.

[103] Only regarding infiltration operations, see Law n.º 12.850/2013, available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. [9 August 2016].
[104] Insufficient information available from country report.

As described at the beginning of this study, Sweetie is an AI tool developed to facilitate the work of law enforcement agencies in online operations. As an AI agent, the chatbot would operate in open (public) online systems without direct human intervention, thereby enjoying a certain autonomy in conduct. Further, the chatbot/avatar will be used as a lure for the alleged offender, but will also be capable of interacting with the suspect and recording and storing their interactions as well as available information on the offender, such as for instance his IP address.

The use of Sweetie as an investigative tool is not specifically covered in any of the jurisdictions in this study. In fact, no explicit rules exist on the use of AI agents for the purpose of criminal investigations. However, undercover investigations usually make use of a number of technical tools and coercive powers that resemble Sweetie's features. For instance, when placing a lure, law enforcement may either use physical objects, such as cars or bikes (or other goods depending on the crime), or stage an officer with a fake identity. Undercover agents that interact with suspects within a criminal organisation also make use of fake identities and usually do so in the framework of an infiltration operation. Further, in order to get access to the suspect's communications, state agencies use wiretapping and interception devices, and additional technological means capable of processing and storing the obtained data. Accordingly, given the lack of similar examples and against the background of its technical features, for the purposes of the present study the chatbot will be characterised and dealt with as a 'hybrid' investigation tool that combines the capacities of the different investigative tools mentioned above.

4.5 Authorised use of Sweetie by law enforcement

The fact that Sweetie is a new investigative technique and existing investigative powers do not explicitly refer to any software or technology comparable to it, does not *per se* exclude the use of AI for investigative purposes. The use of the chatbot is possible as long as its application stays within the boundaries established by the law.

As Sweetie is designed to identify and engage suspects in a manner comparable to undercover investigators, the rules regulating the latter will be decisive for its application. Further, the chatbot will collect certain information on the alleged offender and its devices, and store the content of the communications between that person and Sweetie for investigation purposes. Consequently, the rules authorising these different investigative powers would conjointly be applicable in the case of the chatbot.

Whether the use of Sweetie is allowed depends on an answer to the following questions:

1) Does Sweetie lead to a substantial risk of infringement of human rights in the context of a criminal investigation?[105]

If so,

[105] If the answer to this question is negative, than there is no need to further question and codify the use of Sweetie as an investigative method from a human rights and criminal law perspective.

2) Is the use of Sweetie 'necessary in a democratic society'?

3) Is the use of Sweetie 'in accordance with the law', that is to say, should there either be a specific legal basis regulating its use, or should its use be otherwise governed by procedural requirements?

Below we will answer these questions.

4.6 Possible human rights infringements through Sweetie

Before we discuss the investigative powers that might come into play when regulating Sweetie, we need to establish whether a specific investigative power is actually necessary. This means determining whether and how human rights infringements may take place when using Sweetie. When we observe the use of Sweetie, two fundamental rights of suspects may be particularly at risk:

1) privacy (given that Sweetie may engage in conversations and record any communications), and
2) the right to a fair trial (given that Sweetie may entrap suspects).

If these rights are infringed upon by using Sweetie, a specific investigative power that satisfies the procedural guarantees of legality, proportionality and subsidiarity would have to be in place.

4.6.1 Privacy

The right to privacy is recognised throughout the world. Even though with differing degrees of relevance, both in common and civil law traditions distinctions are made between the public sphere and the private sphere, and case law has evolved to facilitate the differentiation. It is generally held that in the public sphere, a suspect has less of a reasonable expectation of privacy. The level of protection provided though differs from jurisdiction to jurisdiction.

Australia, for instance, has a comparatively undeveloped right to privacy.[106] The cogency and relevance of the obtained evidence is usually prioritised over the privacy interest of the suspect even if said evidence has not been obtained in a public communication. Under the ECHR, on the other hand, persons can have a privacy interest in the public sphere, in particular when their behaviour is recorded.[107] Under the US Constitution, however, a reasonable expectation of

[106] Australia does not have a constitutional Bill of Rights, which impacts the scope of the *due process* protection of the suspect. The common law protection against excessive privacy intrusions is more property-oriented, and usually the threatened public interests trump the individual ones. For instance, in the case of O'Neill v R ([1995] 81 A Crim R 458) the court considered the use of listening devices a desirable methodology against the risk of untrue confessions by untrustworthy informers, instead of raising privacy concerns and how these affect the suspect's interests.

[107] See e.g. Von Hannover v Germany, Application no. 59320/00, and Peck v United Kingdom, Application no. 44647/98.

privacy in public spaces and with regard to information divulged to third parties is more limited.[108]

Yet, while the distinction between public and private is relatively straightforward in the physical world, it is much less so on the Internet. This raises questions with regard to the use of Sweetie by law enforcement.

Whether or not Sweetie's use would lead to a substantial infringement of the suspect's privacy rights depends on the particular circumstances of the case. When it comes to Sweetie we can distinguish two situations from a privacy perspective: 1) Sweetie being present in a public chatroom, and 2) Sweetie directly interacting with a suspect one-on-one in a private (video)chat.

Sweetie being present in a public chatroom

With regard to Sweetie merely being present in a public chatroom, the privacy infringement seems limited. But of course Sweetie just being present does not yet serve a clear law enforcement purpose. This may change though if Sweetie records (logs) the conversations in the chat. In these cases, there might be a substantial infringement of privacy. However, as it stands this is still the subject of debate.[109]

In general, information that is made publicly available on the Internet may be gathered by law enforcement as evidence in a criminal investigation without the need for a specific legal basis.[110] However, the question becomes more difficult if the information is stored, or if publicly available information is monitored for an extended period. In these cases, the privacy infringements may be of a different nature, because the scope, scale and duration are different when compared to offline cases. In the jurisdictions examined, there is as of yet limited case law or specific legislation governing this issue. In the Netherlands, for instance, there is an ongoing discussion to what extent open source data (e.g. blogposts, public Facebook profiles, Twitter feeds) may be monitored on a more structural basis.[111] A similar debate can also be witnessed in the UK, accentuating that reading something that is behind password protection, even if its end result is an open source post, would normally engage privacy expectations covered by Art. 8 ECHR.[112]

In any case the goal of Sweetie 2.0 is not to monitor public chatrooms and discussions. Rather, Sweetie is deployed as a lure in the public chatroom in order to engage with potential child sex offenders. As such, the possible privacy infringements that take place in the context of one-one-one conversations and interactions are likely to be more relevant.

One-on-one conversations and interaction

[108] See e.g., Katz v United States, 389 U.S. 347 (1967), United States v Miller, 425 U.S. 435, 443 (1976), Smith v Maryland, 442 US 735, 744 (1979); Hoffa v United States, 385 U.S. 293, 302 (1966); Lopez v United States, 373 U.S. 427 (1963).

[109] See for instance Koops, BJ 2013, 'Police investigations in Internet open sources: Procedural-law issues', *Computer Law & Security Review*, *29*(6), pp. 654-665.

[110] See for instance US country report, section 3.4.1, p. 22.

[111] Koops, BJ 2013, 'Police investigations in Internet open sources: Procedural-law issues', pp. 654-665.

[112] England and Wales report, section 3.3, p. 46.

Once Sweetie has been approached for a chat there is the possibility to log the conversation (text, audio and video). These chats can subsequently be used as evidence.

Private chatrooms and one-on-one conversations are generally regarded as more privacy-sensitive.[113] Participating in or eavesdropping on conversations as law enforcement official is generally considered an interference with the suspect's private life, requiring the use of special investigative powers subject to authorisation by a public prosecutor or (investigative) judge.[114]

Personal communications and information stored on or transmitted through personal electronic devices are generally protected by the right to privacy[115] as described in amongst others, Art. 17 ICCPR, Art. 8 ECHR and the 4th Amendment to the United States Constitution. These instruments protect the individual's 'freedom from unwarranted and unreasonable intrusion into activities […] belonging to the realm of individual autonomy'.[116]

An interference with the right to privacy may be justified under Art. 8 (2) ECHR as long as the public authority's actions are 'in accordance with the law' and 'necessary in a democratic society' and pursue 'legitimate aims'. The 'legitimate aims' include, among others, also crime and disorder prevention and protection of the rights of others. Art. 17 ICCPR does not include an explicit constraint clause, providing instead that 'no one should be subjected to arbitrary or unlawful interference'. In the years of practice the two bodies guarding the conventions, the ECtHR and the HRC respectively, have aligned their approaches and have established very similar assessment criteria of how a permissible limitation of the right looks like.[117] They examine in the first place whether the interference with the individual's privacy is lawful/in accordance with the law, which means that the investigative power in question should have a proper legal basis. They further consider criteria of proportionality and subsidiarity that must be satisfied as well.

The tests of legality, proportionality and subsidiarity have been widely translated into the criminal systems of the studied countries.[118] Following its considerations, most of them have enacted legislation that allows law enforcement to (temporarily) infringe upon privacy rights

[113] See Koops, BJ 2013, 'Police investigations in Internet open sources: Procedural-law issues', pp. 654-665.
[114] A notable exception is the United States. US citizens have no reasonable expectation with regard to information they voluntarily disclose to another person, even if this person turns out to be an undercover law enforcement agent (see e.g. Hoffa v United States, 385 U.S. 293, 302 (1966)).
[115] Art. 8 ECHR uses the term 'private life', while Art. 17 ICCPR speaks of 'privacy'. Here both terms are used synonymously, as despite the linguistic differences in the two English texts it is widely recognized that 'privacy' and 'private life' mean the same thing.
[116] Wilborn, SE 1997, 'Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace', p. 833.
[117] Georgieva, I 2015, 'The Right to Privacy under Fire Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR', p.104.
[118] In Brazil, the right to privacy is constitutionally guaranteed and said guarantee can be temporarily suspended in matters of public interest, especially in criminal investigations with judicial authorization. The investigative authority in Canada is constrained by the Canadian Charter of Rights, and in particular by its s.8 that covers the freedom from unreasonable search and seizure, from which the common law has deduced a right to privacy and a doctrine of reasonable expectations of privacy. See also Section 26 (2) of the Estonian Constitution and Articles 10 – 13 of the Dutch Constitution. In Israel, the constitutional limitations of investigative powers are comparatively weak, see country report on Israel, p. 14. In Spain, respect for the right to privacy and the confidentiality of communications is reflected in the guiding principles of Art. 588bis a). The Nigerian Constitution guarantees the right to privacy (Section 37), but it is not absolute and can be restricted (Section 45 (1) of the 1999 Constitution).

of citizens for investigative purposes.[119] In most cases, an independent body is to authorise the measures of a more intrusive character provided that the latter have already been enacted and specified by the law.[120] The criminal procedural laws thus clearly distinguish between intrusive and less intrusive investigation powers, the latter of which do not always require a specific legal basis.

In summary, we can say that Sweetie may indeed infringe the privacy of suspects, and will do so in particular in one-on-one conversations, and even more so if such conversations are logged/recorded. Therefore, its use must both be necessary in a democratic society and in accordance with the law. This will be further analysed below (see s. 4.7 and 4.8).

4.6.2 Fair trial (entrapment)

In the context of criminal procedure, the right to a fair trial protects individuals against arbitrary application of state power, and guarantees the effective realisation of other fundamental rights and liberties through fair judicial proceedings.[121] Fair trial rights may also extend to the pre-trial phase. Consequently, it also covers situations in which law enforcement officials use a fake identity, simulate a sale or purchase, or offer simulated business services to trap a suspect, as in such cases the suspect's fate is 'surrendered' to the power advantage of the state. The right to a fair trial and its considerations balance the power relation between the individual and the state.

From a procedural law perspective, the use of Sweetie for engaging suspects raises two issues regarding the fair trial rights of the suspect. They are: 1) operating Sweetie in public chatrooms upon a general suspicion may constitute non-targeted entrapment that is considered random virtue-testing, and 2) its direct interaction with suspects may amount to unlawful incitement of crimes.

---

[119] Under Croatian law it is Art. 332 of the Criminal Procedure Act; s.111 of the Estonian Electronic Communications Act (ECA).

[120] In a recent landmark case, R v Spencer [2014] 2 SCR 212, 2014 SCC 43 (CanLII), the Supreme Court of Canada held that subscriber information can no longer be obtained by the authorities from Internet service providers without a corresponding court authorization. Art. 332 of the Criminal Procedure Act of Croatia stipulates that restrictions of privacy rights can be legally implemented only upon a court order, leaving the state attorney a discretion to issue a warrant in urgent cases for the duration of 24 hours. See Croatian report, pp. 25-27. In Belgium, according to Art. 88*bis* and Art. 88*ter* CCP the intervention of the investigatory judge is necessary whenever traffic or localization data is required, or when a network search has to be performed. In England and Wales, S.65 (1) RIPA has (controversially) created the Investigatory Powers Tribunal, which supervises the techniques awarded by RIPA to police and security services. In Argentina, a judicial authorization is needed whenever investigatory powers imply a violation of privacy rights, see Salt, M and Dupuy, D, *Substantive and procedural legislation in Argentina to combat webcam-related child sexual abuse* (Country report on Argentina), section 3.2.2. In Australia, the statutes mirror the protection thresholds of the Cybercrime Convention on personal information by, among others, requiring a warrant to allow access to existing or prospective computer data, see country report on Australia, pp. 21-23. In Brazil, it is also the judicial authority that is considering the proportionality of the measure and the factual reasoning supporting the request for an interception warrant. In Nigeria, law enforcement authorities must obtain judicial authorization before carrying out an interception, see s.39 of the Cybercrimes Act. The 1987 Constitution of the Philippines foresees in its Art. III sec 3 (1) a judicial warrant or a court order as well. The Polish Code of Criminal Procedure balances investigative powers with the requirement of a court order as well, see Art. 237 CCP and Art. 218 CCP. In the US, under the Fourth Amendment, law enforcement must generally obtain a warrant in order to conduct a search in a computer owned by the suspect, see US country report, p. 15.

[121] Ballin, MFH 2012, *Anticipative Criminal Investigation*, p. 55.

1) Operating Sweetie in public chatrooms
Operating Sweetie upon a general suspicion means that the avatar would not target a particular suspect, but an area or space (in the present case particular cyber-areas such as chatrooms). This raises concerns in terms of the fair trial rights of the suspects, as undercover powers are usually the exception to the rule, and generally aimed at suspects against whom there is a prior suspicion.

2) Direct interaction
A further concern is Sweetie's interaction with the suspects in chat conversations. A direct interaction bears the risk of influencing the suspect and thus leading him/her into committing an offence he/she would have otherwise not committed. Consequently, Sweetie may lead to the facilitation of the crimes it actually intends to prevent.

In both scenarios (use in public chatrooms and direct interaction) there is a risk that the right to a fair trial is violated.

4.7 Necessity in a democratic society

From the above we can surmise that Sweetie brings with it the risk of privacy infringement. As such, it is important to determine whether or not the use of Sweetie is necessary. In other words, does the end (protecting children) justify the means (using an AI to engage suspects and potentially infringe upon their rights)?

The substantial test of 'necessary in a democratic society' is in the centre of the discussion when assessing whether states are allowed to interfere with individual interests in order to address relevant societal matters. This means that when state agencies use infringing investigative powers, just *a* reason for using the power is not sufficient, as the interference must be 'necessary'.[122] The ECtHR in its case law has clarified what 'necessity means':

> *... the notion of necessity implies that an interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued.*[123]

Proportionality is considered an essential test in relation to criminal procedure, especially when courts are assessing the appropriateness of governmental measures, such as secret surveillance operations, interception and wiretapping that interfere with the individual's right to privacy and private life protected by Art. 8 ECHR and Art. 17 ICCPR.

The ECtHR considers the proportionality of the measure in the light of the specific circumstances as a whole, and in particular whether the authorities had 'relevant and sufficient reasons' for taking the coercive measure in question.[124] The process of deciding includes a number of factors, among others, the suspect's interest to be protected from the interference with his/her rights, the severity of the infringement and the pressing social need the authorities seek to fulfil. The more far-reaching the interference is, the stronger the reasons required to

[122] *Handyside v the UK*, Application no. 5493/72.
[123] *Olsson v Sweden*, Application no. 10465/83.
[124] *Olsson v Sweden*, Application no. 10465/83.

justify it must be.[125] The Court, however, affords states a certain margin of appreciation[126] in choosing the means to best address the urgent needs of their society, and said margin of appreciation has a different scope depending on the actual circumstances and the subject matter. It has been held to be particularly wide in areas such as child protection.[127]

In addition, in cases dealing with children and vulnerable groups, the ECtHR has found that positive state obligations can trump negative ones when it comes to securing the physical and moral welfare of children.[128] In said scenarios, states are required to have in place effective criminal law provisions that would not only protect minors, but also effectively deter against grave acts committed towards them.[129]

Considering the above, in order to deem the chatbot's use necessary in a democratic society, the interests it seeks to protect should outweigh the interests of the potential suspects it would investigate. This means that the rights and interests of children who are or could potentially fall victim to webcam sex abuse should outbalance the interests of people who engage in a private chat conversation with the avatar. Furthermore, less infringing cannot yield the same results.

The threat webcam sex tourism poses to the well-being of children is clear. Webcam sex sessions directly hurt the victim, and the fact that webcam streaming sessions can easily produce pictures or videos of the victims, causes additional harm. Furthermore, recorded abuse images and videos can easily lead to the subsequent distribution of child pornography, causing additional harm to the child.

The threshold to engage in webcam sex tourism is low and the chances of getting caught are as of yet minimal. Perpetrators can further reduce the chances of being caught by using fake identities, but also various anonymisation services and hidden servers (to name just a few) to prevent detection. As such, the chances of identifying a suspect after the webcam sex stream has been concluded is likely low. The best chance of finding a suspect, is thus to catch them in the act. This entails luring the suspect, and subsequently interacting with them. While this can be done using actual law enforcement officers, the scale of the webcam sex tourism problem means that this 'traditional' way of investigation is not effective. In order to effectively combat webcam sex tourism, the use of scalable investigation methods such as Sweetie may therefore be necessary.

It is important to consider that the chatbot does not indiscriminately collect all available information in public chatrooms, but only records communications with, and gathers data of, suspects who engage the avatar in a sexually charged conversations. By facilitating the offender's identification, the chatbot would contribute to the effective investigation of serious crimes against minors, which in its turn corresponds to the ECtHR's standards on proactively defending vulnerable groups by effective and deterrent criminal procedure means.

[125] Kilkelly, U 2003, *A guide to the implementation of Article 8 of the European Convention on Human Rights. Human rights handbooks Nr. 1*, p. 34
[126] *Klass and others v Germany,* § 48; *Leander v Sweden,* App no 9248/81, § 59.
[127] Kilkelly, U, p. 34.
[128] See *KU v Finland*, Application no. 2872/02, § 46.
[129] Ibid at § 43.

In line with the above, the question of prioritising the investigation of such offences by means of the chatbot seems necessary to successfully police public chatrooms, and other online venues for child sexual abuse, and fight the online abuse of children. The lasting harm experienced by minors in cases of sexual abuse combined with the ever-growing danger of webcam sex in public chatrooms tips the balance in favour of Sweetie. Minors need to be safe to freely express themselves on the Internet without being monitored by offenders.[130] As such, we argue that depending on the circumstances of the case, there are strong arguments that the use of Sweetie is necessary in a democratic society.

4.8 Legitimacy of the use of Sweetie

Having established that Sweetie can potentially interfere with the right to privacy means that such an interference has to be covered by an investigative power, which requires a clear legal basis. None of the jurisdictions we examined have specific legal provisions that authorise and govern the use of Sweetie. Rather, the use of Sweetie must be 'read' into the existing investigative powers. When translating the existing investigative powers into the context of Sweetie, their interpretation has to match the rationale of the original provisions. A too far-stretched interpretation would contravene the legislator's will, but also rob the provisions of their foreseeability.

It is dependent on the criminal procedure law provisions of the individual country whether or not the application of Sweetie is in accordance with the law. However, drawing inspiration from amongst others the Cybercrime Convention and the European Convention on Human Rights we can give an indication of 1) what special investigative powers could apply in relation to privacy, and 2) what procedural requirements must be followed in the case of entrapment.

4.8.1 Privacy considerations

As briefly discussed above, the situation in which Sweetie is merely present in a chatroom is not yet a substantial infringement of privacy. Incidental observation and/or recording of public data will likely also not yet amount to a substantial infringement of privacy. Provisions such as those of Art 32 (a) of the Cybercrime Convention and domestic regulations regarding the general tasks of law enforcement could cover this.

However, if Sweetie starts systematically observing profiles and recording public chats (regardless of the chatroom it is present in), and particularly if she moves onwards to one-on-one conversations, then this could amount to a substantial infringement of privacy that requires a specific basis in the law in many jurisdictions.

Articles 16 through 19 of the Cybercrime Convention are not really applicable to the case of Sweetie.[131] Art. 20 (the real time collection of traffic data) and Art. 21 (the real time collection

[130] Vendius, TT 2015, 'Proactive Undercover Policing and Sexual Crimes against Children on the Internet', p. 18.

[131] The articles regulate the expedited preservation of stored computer data and traffic data, production orders and the search/ seizure of stored computer data respectively.

of content data) could be relevant in the context of Sweetie, given that Sweetie may record both traffic data (e.g. IP addresses) and content data (e.g. chats and files sent).

One complicating factor might be the definition of communications: not all jurisdictions may consider a person interacting with a chatbot to constitute 'communication', if this is interpreted as exchanging of messages between persons. Whether use of Sweetie is or can be interpreted as recording of communications therefore may depend on the specifics of national law. However, since many countries also consider interacting with a machine to be communications, where the machine (e.g., an ATM) can be seen to serve as a proxy for a person (e.g., a bank),[132] we will consider interactions with Sweetie to constitute communications, where the chatbot serves as a proxy for the investigation officer putting it into operation.[133]

The explanatory report to the Cybercrime Convention gives a broad definition of 'interception and 'technical means' that could also cover the use of Sweetie:

> *Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes.*[134]

As such, the signatories to the Cybercrime Convention should already have in place legal provisions that could be applied in the context of Sweetie, at least for offences related to child pornography. Table 6 confirms this assumption.

In the few countries not party to the Convention, however, we see a divergence in how the real-time interception of communications is dealt with. Argentina and South Korea, for instance, have not developed a formal distinction between traffic and content data yet, but refer to both types of communication information as 'data'. Further, these jurisdictions have not enacted particular legislation on real-time data collection and apply therefore the existing provisions on telephone wiretapping accordingly. The latter applies for Brazil and the Philippines which, although having introduced comprehensive legislation on cyber-investigation powers not so long ago, also lack provisions on real-time collection of both traffic and content data.[135] Among

---

[132] Cf. *Explanatory report to the Convention on Cybercrime*, § 227, which identifies visiting a website to be communications in the context of the power of collecting traffic data, and by extension (see § 230) also of interception.

[133] Since interception of communications is often regarded to be one of the most intrusive investigation powers (see, e.g., the Cybercrime Convention), if a jurisdiction conceptualises interactions with Sweetie as non-communicative, then presumably some other, less intrusive, investigation power may be applied to the situation.

[134] *Explanatory report to the Convention on Cybercrime*, § 54.

[135] See Mendes Saldanha, P, *Substantive and procedural legislation in Brazil to combat webcam-related child sexual abuse* (Country report on Brazil), pp. 20-21; See also Dizon, MA, *Substantive and procedural legislation in the Philippines to combat webcam-related child sexual abuse* (Country report on the Philippines), p. 31. Brazil applies the provisions of the *Wiretapping Act* accordingly, while the Philippines rest to the rules on search and seizure.

the non-signatory countries, Nigeria is the only example with explicit legislation on the matter.[136]

However, as telephone interception and wiretapping practices are largely comparable to the interception of online communications, these countries may still meet the legality requirement, if the application of the respective national norms to investigative means comparable to Sweetie has been confirmed by the courts. Yet, in situations in which suspects engage in conversation with the avatar, this will likely not be (fully) covered by the norms regulating the interception/ management of data, but will also largely depend on the rules surrounding the use of undercover agents. Therefore, and for the sake of comprehensiveness, the applicability of the wiretapping norms mentioned above will be discussed together with the laws on undercover agents under section 4.8.3.

4.8.2 Fair trial considerations (entrapment)

In the following, we provide an overview of the criteria used by the investigated jurisdictions to draw a line between permissible luring and not-permissible entrapment. Entrapment is ordinarily an issue relevant in court proceedings, and as such not part of an investigative power. Depending on the particular system and the facts of the case, it can be pertinent in various ways – it can either lead to the exclusion of the obtained evidence,[137] be raised as a defence and thus exclude guilt or liability,[138] or even entirely stay the proceedings due to an abuse of process.[139]

As indicated above, Sweetie brings about issues of both targeted and non-targeted entrapment. This means that in both cases certain procedural requirements must be met that have been established in case law.

4.8.2.1 Targeted entrapment

The compared criminal systems employ as a central consideration of whether unlawful entrapment has actually taken place, the reasons underlying the operation and the conduct of the authorities executing it. It is generally recognised that law enforcement officials are entitled to merely provide the suspect with an opportunity to commit the crime, but the latter should have been able to independently form or abandon the intention to commit it.[140] The suspect

[136] S. 39 (a) of the Cybercrimes Act allows law enforcement to intercept content data and/or traffic data provided that the operation has been authorised by a judge.

[137] As for instance in Australia - see section 138 of the *Evidence Act 1995* (Cth), available at http://www.austlii.edu.au/au/legis/cth/consol_act/ea199580/. [23 May 2016]

[138] This is the case in the US system. See country report on the US, section 3.2.3, p. 16; In Spain entrapment is a judicially crafted defense, which excludes liability. See on the matter SSCS April 18, 1972 and SSCS June 22, 1950.

[139] *R v Loosely Attorney General's Reference (No 3 of 2000*) is considered the landmark decision in the UK establishing entrapment as a procedural bar; Canadian courts also make use of procedural bars, see R v Mack, [1988] 2 SCR 903, as well as their counterparts in Scotland - Jones v HM Advocate [2009] HCJAC 86, para 88.

[140] In Dutch criminal procedure this approach is known as the Tallon criterion, named after a landmark case from 1979 (HR 4 December 1979, NJ 1980, 356 m.nt ThWvV). The case concerned drugs purchase from two undercover agents. The Supreme Court found that the suspect had formed his intent independently. The Belgian general prohibition of entrapment is embedded in Article 30 of the Preliminary Title of the Code of Criminal Procedure and declares criminal procedures based on entrapment inadmissible. In the UKdaniss *R v Loosely Attorney General's Reference (No 3 of 2000*) the crucial question was whether the police have done more than present the defendant with an unexceptional opportunity to commit a crime. A criminal court would consider admissibility under section 78 Police and Criminal Evidence Act 1984 (PACE).The Estonian Supreme Court has

should have been thus 'allowed' to commit the crime he/ she intended to from the very beginning.

The ECtHR refers to this requirement as the '*essentially* passive'[141] standard and examines whether the suspect has in any way experienced pressure by the authorities' deceit to commit the crime, be it by pro-active solicitation,[142] prompting or reiteration of the offer despite an initial refusal,[143] or by making the offer very hard to refuse[144]. The Court also considers whether there were objective indications that the suspect has been involved in criminal activity or was predisposed to commit the crime[145], and how familiar the latter is with the criminal environment.[146]

This reasoning, however, is not unique to the ECtHR or European courts in general. The Canadian[147], Australian[148] and South Korean[149] courts have adopted similar approaches in outlining entrapment, stipulating that law enforcement should not go beyond offering an opportunity by crossing the line and creating the offence for the purpose of prosecuting it. The Supreme Courts of Argentina and the Philippines[150], although phrasing their entrapment tests in slightly different terms, also see the difference between lawful trapping and unlawful entrapment in the origin of the criminal intent. The legal doctrine in Nigeria appears to be developing in a similar direction.[151]

The common law doctrine of the United States considers the predisposition element of the suspect together with the trickery, persuasion or fraud techniques performed by the law enforcement officers (or private persons acting on behalf of law enforcement).[152] According to the so-called subjective approach, entrapment is committed when law enforcement has induced the crime and the defendant had no predisposition to engage in a criminal conduct.[153]

established in its judgement of 2 December 2004, case number 3-1-1-110-04, para 11.3 that the authorities' actions cannot be directed against persons who did not have the slightest intent of committing a crime. The Supreme Court of Croatia considers the persistent, long-term prompting of the suspect incitement when it turns out to be the decisive factor in forming the perpetrator's will to commit the crime, VSRH, I Kž-1255/04 of 16 February 2006.

[141] *Ramanauskas v Lithuania* [GC], Application no. 74420/01, § 55. Emphasis added.

[142] *Burak Hun v Turkey*, Application no. 17570/04, § 44.

[143] *Ramanauskas v Lithuania* [GC], § 67.

[144] *Malininas v Lithuania*, Application no. 10071/04, § 37.

[145] *Bannikova v Russia*, Application no. 18757/06, § 38; *Case of Constantin and Stoian v Romania*, Applications nos. 23782/06 and 46629/06, § 55; *Texeira do Castro v Portugal* (44/1997/828/1034), §§ 37-38.

[146] *Shannon v the United Kingdom,* Application no. 67537/01.

[147] Supreme Court of Canada, R v Mack [1988] 2 SCR 903. In this particular case the Court stayed the proceedings.

[148] See R v Priest [2011] ACTSC 18 at [86] and Ridgeway v The Queen [1995] CLR 19, in which the court rejects a defense of entrapment.

[149] For the South Korean doctrine see for instance Supreme Court Decision, 2008DO7362, Oct 23, 2008.

[150] *Araneta v Court of Appeals*, G.R. No. L-46638 [July 9, 1986]; *People v Gatong-o*, G.R. No. 78698 [December 29, 1988].

[151] See country report on Nigeria, section 3.2.3, p. 46.

[152] See country report on the US, p. 16. In the US, the defense of entrapment has no statutory basis in Federal law, but has been developed by the courts.

[153] *Mathews v United States*, 485 U.S. 58 (1988).

4.8.2.2 Non-targeted entrapment

The case law and regulations discussed above relate to targeted entrapment, but scenarios in which law enforcement officials do not engage a particular suspect and operate upon a general suspicion need to be considered as well. The issue with said conduct is that it may be considered 'random virtue-testing'[154] that puts the integrity of the criminal investigations at risk. Criteria that govern non-targeted operations must therefore be in place.

The studied jurisdictions show, however, somewhat more perceptible differences in their approaches towards non-targeted entrapment. While in Australia, the Philippines, Poland, the UK and the US the fact that law enforcement targets a location or an area, but not a person, triggers the application of the same criteria as described above, other criminal procedure codes, as the one in Croatia for instance, limit the use of special investigatory tools to cases where a particular person has already been identified as a suspect.[155] Yet, the deployment of undercover agents would be legally permissible under the Croatian Law on Police Duties and Powers, which allows location-related undercover operations provided that there are valid grounds for suspicion of criminal behaviour. Similarly, Canada's doctrine also provides additional safeguards in this regard. Where undercover operations concern a particular place or a location, but not a given suspect, the authorities must reasonably suspect that criminal activities are occurring there. The police activity must either take place on the basis of a reasonable suspicion or over the course of a *bona fide* inquiry. In this way the doctrine ensures that no random virtue-testing is being practiced.[156] Scottish law requires state agents to obtain an authorisation before executing an operation when the suspects are not identified.[157]

Yet other approaches focus on the ordinariness of the law enforcement behaviour. Following the *Tallon criterion*[158] in the Dutch procedural context, non-targeted entrapment would be allowed if the lure does not substantially change the original situation or location in which it is employed, so that it cannot exert any significant impact or influence on the decision-making process of the suspect.[159] The Belgian Court of Cassation handles non-targeted entrapment in a similar manner. The decisive criterion in their view is that the luring procedure imitates or portrays a daily life scene without exaggeration.[160]

4.8.2.3 Fair trial requirements applied to Sweetie

Considering the substantive entrapment tests outlined under section 4.8.2, Sweetie's conduct must remain essentially passive to avoid investigative impropriety. Further, once the suspect has been engaged in a conversation, the chat script should also leave room for the suspect to retreat. If the avatar does not proactively solicit potential suspects, but waits to be approached, and avoids pressure or any inducement to steer the conversation in a particular, sexually

---

[154] Bronitt, S 2004, 'The law in undercover policing: A comparative study of entrapment and covert interviewing in Australia, Canada and Europe', p. 37.
[155] See Art. 332 (1) and Art. 334 of the Criminal Procedure Act of Croatia.
[156] See Supreme Court of Canada, R v Mack [1988] 2 SCR 903, paras 113, 119.
[157] See country report on Scotland, p. 21.
[158] Ibid at fn. 140.
[159] These contemplations originate from two important cases of the Dutch Supreme Coourt, HR 28 oktober 2008, ECLI:NL:HR:2008:BE9817 (*Lokfiets-arrest*) and HR 6 oktober 2009, ECLI:NL:HR:2009:BI7084 (*Lokauto-arrest*). In both cases bait was set by law enforcement without suspicion of a specific person.
[160] Cass. 17 maart 2010, AR P100010F; Brussel 14 maart 2007, *RABG* 2008, afl. 1, 63, note L. Delbrouck.

charged, direction, it would act beyond legal reproach. It appears that an exception to this test can only be made within the US framework, where courts are likely to close an eye on a more provocative behaviour, if the suspect has a demonstrable predisposition towards child abuse offences.[161]

Further, with regard to the location of the undercover operation, that is to say when it targets an area (presently a chatroom) and not a particular suspect, it is relevant that the use of the chatbot does not significantly alter the existing circumstances. This, of course, would be largely dependent on the targeted chatroom.

If Sweetie is used in a regular chatroom for users under the age of 18, and her profile resembles that of the majority of minors there, her online presence would abide by this rule, if it does not make itself more visible than the mere entering a chatroom with a common-looking chat name. In addition, for some of the jurisdictions described above,[162] law enforcement agencies would need to substantiate their initial suspicion or get a particular authorisation from an independent body to proceed with a non-targeted operation in a chatroom. Disregarding these criteria would likely compromise the admissibility of the gathered evidence or of the investigation as a whole.

If, however, Sweetie enters an 'above 18' chatroom, already her logging-in is likely to significantly alter the situation. In such cases, the particular assessment of the avatar's placement will depend among others on the number of real children present there. While there might be indeed some room to employ the chatbot in online areas intended as 'adults only'-fora, but demonstrably being used for the webcam prostitution of real children, Sweetie's appearance in a regular adult chatroom would likely constitute non-targeted entrapment.

An additional question arises in relation to recurring offenders (persons returning to the same chatroom and repeatedly engaging the avatar in a sexually charged conversation) and whether a different entrapment test (or a suspicion threshold for that matter) should apply to them, since the chatbot would be 're-encountering' them. However, as of the writing of this report, there is no information that such situations are being handled differently. It appears that the rules on non-targeted entrapment are applicable in such cases as well, especially since the avatar's presence in the chatroom would not aim to engage offenders with whom the chatbot has already communicated, but potentially everyone who has an interest in an illegal webcam interaction with a child.

It is, however, doubtful whether we can adequately assess Sweetie's entrapment implications at all, since the entrapment tests discussed above have their origin in police operations, which are substantially different from online investigations of sexual exploitation. This in its turn is closely connected to the question of Sweetie's authorisation as an investigation tool, which will be discussed shortly.

Although some entrapment tests refer to the situation of placing an opportunity for potential suspects in 'hotspot' areas, said techniques merely stage a (conventional) subject in an everyday environment (a car, a bike or even a person in a park that however does not interact),

[161] See US country report, p. 18.
[162] See the references made under section 4.8.2.2 of this report.

which does not require further police intervention until the suspect takes the bait. Sweetie, however, seems to exceed this mandate, as it will undeniably interact with the suspect. As such, Sweetie resembles more an undercover agent, and its interactive capacity would fall under the authority of more comprehensive undercover operations, which typically involve pseudo-purchases of illegal goods (the so-called *buy and bust* approach), the infiltration of a criminal environment or both at the same time. In these scenarios undercover agents are allowed to act as offenders or to be in direct contact with offenders, and thereby to actively take part in the crime (if national law allows such operations, e.g., for drugs investigations).

Yet, these controlled operations start from preconditions that differ from Sweetie. Sweetie does not act as an offender, but as an 'interacting' child victim. Accordingly, the rules on undercover operations in which police act under a false identity while posing as a victim would apply. Here, considering the chatbot's mandate to tackle webcam child sex tourism on a global level, it is pertinent to establish whether there is any international legislation that can guide undercover agents in such operations.

In the European context especially, the EU has long proactively sought to find a solution to streamlining particular undercover techniques, including the use of undercover agents and their operational capacities.[163] The European Investigation Order (EIO)[164] reflects said objective, and Art. 29 stipulates:

> *An EIO may be issued for the purpose of requesting the executing State to assist the issuing State in the conduct of investigations into crime by officers acting under covert or false identity ('covert investigations').*

However, the article also clearly establishes that covert investigations should take place 'in accordance with the national law and procedures of the Member State on the territory of which the covert investigation takes place'.[165] In other words, the use of undercover agents remains a strictly national matter.

In terms of other international instruments on undercover agents, at the time of writing this report, no binding guidelines exist. Further authorisation is thus to be sought in the country specific norms on investigative powers.

4.8.3 Overview of country-specific rules in relation to privacy and entrapment

In Argentina, the undercover agent figure is codified under Law 24424 (the so-called Drugs Law), but is explicitly recognised only for operations investigating the trafficking or smuggling of narcotics.[166] In addition, there is no general regulation on undercover operations online, or surveillance for that matter,[167] so it appears that investigations concerning online activities resort to the rules on obtaining physical evidence and apply them in analogy. Having said that,

[163] See Vendius, TT 2015, 'Proactive Undercover Policing and Sexual Crimes against Children on the Internet', p. 20.
[164] Parliament and Council Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters.
[165] See Art. 29 Directive 2014/41/EU.
[166] See Argentinian report, p. 23.
[167] Ibid, pp. 23-27.

and considering that under current Argentinian law an inappropriate interaction with Sweetie can only be dealt with under the figure of impossible attempt (which as explained above appears to have no clear assessment criteria),[168] finding a legal basis for the avatar's use seems challenging.

The findings of the Australian report indicate that there are no obvious impediments to Sweetie's investigatory use. The country's regulations on covert policing[169] have been mainly developed to oversee covert operations, in which officers would perform otherwise unlawful acts, such as the delivery of narcotics. Covert online investigations of child grooming (in contrast to infiltration of online child pornography rings) usually do not require the police to resort to these mechanisms,[170] and no court has ruled on whether it is improper to conduct such investigations without the use of a controlled operation or assumed identity authority in the absence of otherwise unlawful conduct. Following this premise, Sweetie can be used both as a lure and an undercover agent that gathers information. The evidence gathering features of the chatbot would be qualified as a surveillance device.

In Belgium, there are possible avenues for using the chatbot following an evolutionary interpretation of the provisions on infiltration and wiretap operations.[171] These, however, are not applicable to investigations concerning the offences of cyber-luring and cyber-grooming, which are excluded from the list of offences triggering said investigative powers. Accordingly, law enforcement will have to rely on offences like cyberstalking (Art. 145, § 3*bis* Act Regarding Electronic Communications) to obtain the necessary authorisation.

Brazilian criminal procedures on the interception of communications, the collection of traffic data and other similar investigation techniques require a court authorisation as well.[172] While it appears that said means have been used in the course of operation 'Darknet', known for successfully bringing child pornography offenders to justice, the details of the investigation are still sealed.[173] It is therefore difficult to find examples of their application in an online environment. In addition, while the law on infiltration operations[174] can also be taken into consideration as authorisation for Sweetie's recording of webcam streams and chat logs, employing Sweetie as bait is considered illegal. Further, as a crime against an avatar cannot be prosecuted in Brazil, there is no legal basis for its investigation either.

S.184(2)(a) of the Canadian Criminal Code, that applies to both wiretapping and undercover operations, regulates the interception of communications where one party consents to recording. Depending on the interpretation of the provision, consent could be reasonably established by Sweetie's operators / the Canadian police. Should that not be the case, a judicial authorisation would be necessary for every instance of Sweetie's interaction with a potential

[168] See section 3.4.2 of this report.
[169] See the *Crimes Act 1912 (Cth),* available at: http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/. [9 August 2016].
[170] R v Priest [2011] ACTSC 18 (11 February 2011) at [90]. See also country report on Australia, p. 24.
[171] Belgian report, section 3.4, p. 37.
[172] See Brazilian country report, p. 25.
[173] Ibid, section 3.4, p. 26.
[174] Law n.º 12.850/2013, Art. n.º 3º, IV, V and VII, and Arts. 10 – 17. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. [9 September 2016].

suspect pursuant to s.184(2)(b) CCC. As for the overall regulation of undercover operations in Canada, these are subject to the provisions on statutory police powers, whose foundation appear to be common law principles and the existing extensive case law on undercover policing.[175] Following their rationale, the legality of Sweetie's use as an undercover agent appears to be quite plausible.

The Croatian Criminal Procedure Act contains provisions on the use of undercover investigators and informants, simulated sale and purchase of items, and simulated bribe-giving and business services,[176] but it makes no explicit reference to the use of software or technologies for investigative purposes.[177] Yet, given that the law on special investigatory procedures allows operations in which undercover investigators set fake profiles on social networks and other Internet fora in order to communicate with potential perpetrators, the use of Sweetie for the same purpose appears possible.[178]

Under English law, the rules on undercover police operation, surveillance and on the interception of content and communications data have been tested in cases where officers would pose as children online, and it appears that said rules provide a sufficient legal basis for Sweetie. Interestingly, under those provisions, since one part of the communication is known (presently Sweetie), exchanging messages between the avatar and the alleged offender would not amount to interception.[179]

The laws on undercover surveillance activities carried out by police agents cover luring and interacting with a suspect in Estonia.[180] Yet, the provisions explicitly refer to a 'police agent', implying the involvement of a human being. This is problematic given that the rules at hand are quite recent, meaning that the laws have been consciously enacted without consideration of virtual undercover agents or other AI technological means, and there is no case law (yet) that would advocate a different interpretation.

Since under Israeli procedural law no provision explicitly authorises law enforcement to employ undercover agents, but police operations make use of such means nevertheless, according to the country report it does not matter whether said unauthorised power is executed in the context of offline or online investigations; nor does it matter whether the police use a human or a computer agent. Therefore, investigation powers in Israel can be applied to Sweetie.[181]

Given that under Dutch law many of the investigatory powers are formulated in a technology-neutral manner, they are applicable to the online context as well.[182] Sweetie's use could fall under article 126g DCCP and 126j DCCP, which regulate systematic observations and the

[175] Said operations are limited by constitutional guarantees and controlled (where necessary) by judicial oversight.
[176] Art 332 (1) point 5, 6 ,7 of the Criminal Procedure Act, Official Gazette no. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14.
[177] However, the law does not exclude them either.
[178] See the findings of the Croatian country report, section 3.4, p. 32.
[179] See report on England and Wales, p. 47.
[180] See section 3.3.2.2.2 of the Estonian report.
[181] See Israeli report, p. 16.
[182] Country report on the Netherlands, section 3.3, p. 24.

method of systematically gathering intelligence online respectively.[183] Further, the investigative method stipulated in article 126m DCCP may also be used in the context of Sweetie, for instance, to record the webcam stream, or the associated chats.

The Nigerian rules that regulate the interception of communications upon a judicial authorization (online observation and electronic infiltration embedded in sections 39 and 39 (b) of the Cybercrimes Act respectively) seem to refer to technological means such as the installation of software or a device, but not to artificial intelligence agents. The conduct of undercover agents is also not explicitly regulated.[184] Therefore, there appears to be no explicit legal basis for using Sweetie in Nigeria.[185]

Under Philippine law, while there seems to be some legal basis for the use of Sweetie as a lure,[186] other investigation practices, such as the search, seizure, preservation and production of computer systems and data, are principally only applicable to cases involving real children. Exceptions can be considered with regard to the few crimes directly applicable to Sweetie, which as indicated above are grooming, luring, cybersex, and attempted cybersex. Short of this, there will be no legal basis for law enforcement to search, intercept or collect data from or about suspected sex offenders, since the latter would not be involved in the commission of any crime.[187]

The avatar's use in Poland can be submitted for one part of the process under article 19a and 19b of the Police Act, which regulate controlled operations or the so-called 'police provocation'[188]. These would govern the avatar's interaction with and luring of the suspect, and cover, for instance, the receipt of material containing child pornography. The collection of information could then fall under article 19 and 20 of the Police Act. They regulate, on the one hand, the collection of the communication's content and its preservation, including webcam footage and other computer data, and the obtaining and processing of personal information on the suspect, on the other.[189] Yet, article 19a and 19b usually authorise operations where a suspect has already been identified, and not to the other way around, which markedly reduces the situations in which Sweetie can be legally used.

Provided that law enforcement obtains the necessary authorisation for undercover operations, Sweetie appears to be usable under Scots law.[190]

[183] These provisions cannot be applied upon a general suspicion. In Sweetie's case, their application would depend on the particular circumstances of the case and on how law enforcement substantiates their conduct.
[184] See Nigerian report, p. 44.
[185] See Nigerian report, section 3.4, p. 48.
[186] The findings in the country report on the Philippines indicate that there are no specific laws on undercover policing and operations. Such activities are subject to general laws (i.e. the rights and protections granted under the Philippine Constitution) and the relevant case law on entrapment. See on the matter section 3.2.3 of the country report.
[187] See country report on the Philippines, p. 36.
[188] See country report on Poland, section 3.4, p. 35.
[189] Both provisions implement a three-step safeguarding system, which requires the approval of the high-rank police officers, the prosecutor and the district court. See for more information the Polish report, p. 35.
[190] See country report on Scotland, p. 21.

In Spain, Sweetie's use will only be possible under article 282bis of the Criminal Procedure Act, which codifies the figure of the so-called cyber-undercover agent. This refers to a police officer who acts under a false identity in an online setting. The provision allows the agent's interaction with a suspect and the recording of the communication, provided that the necessary authorisations have been obtained.[191] However, since under Spanish substantive criminal law a crime against Sweetie cannot be committed and an attempt is not punishable, the chatbot could only be employed as a form of intercepting device against already identified suspects.

In Turkey, article 139 of the Criminal Procedure Code regulates the appointment of undercover agents, while the interception, recording and evaluation of electronic signals transmitted through telecommunication channels are embedded as a method of investigation in article. 135 (1) of the same statute.[192] However, undercover agents may only be used to investigate the crimes listed exhaustively in article 139 (7), which does not include the crimes against the sexual integrity embodied in articles 102-105 or articles. 226-227 of the Turkish Penal Code.[193] In a similar manner, data interception and recording powers are only applicable to article 103 and article 102 (1) of the Penal Code (sexual exploitation of children and sexual assault respectively), the former of which requires physical contact between the offender and the victim, while the latter refers to an adult victim. Considering the above, Sweetie would have no legal basis under the current criminal law framework in Turkey.

The US procedural system allows the recording of private one-on-one chat communications, given that Sweetie could be considered a party to the conversation.[194] As to its authorisation as a lure or an undercover agent, it is likely that courts will simply consider Sweetie a way to automate undercover operations, and the rules that apply to the chatbot are those that regulate undercover operations.[195]

[191] See Spanish report, p. 34.
[192] See country report on Turkey, section 3.4, p. 30.
[193] See country report on Turkey, section 3.2.3, p. 27.
[194] 18 U.S.C. § 2511(2)(d), see also 18 U.S.C. § 2511(2)(c). However, the law speaks of a 'person' and not of an AI agent. It appears that the provisions could be applied to Sweetie if the avatar is seen as a proxy of the law enforcement officer supervising its communication with the suspect. See the country report on the US, section 3.4.1, p. 21.
[195] The rules covering undercover operations have no specific statutory basis, and as a result have been developed by the courts.

Table 7: Applicability of existing investigative powers to Sweetie			
	Explicit laws on AI-investigatory tools	Laws on special investigatory powers	Application of the laws to AIs such as Sweetie
Argentina	-	X	-
Australia	-	X	X
Belgium	-	X	X (for some crimes)
Brazil	-	X	-
Canada	-	X	X
Croatia	-	X	X (no case law yet)
England and Wales	-	X	X
Estonia	-	X	-
Israel	-	X[196]	X
Netherlands	-	X	-
Nigeria	-	X	-
Philippines	-	X	X (for a few crimes only)
Poland	-	X	X (if suspect identified)[197]
Scotland	-	X	X (possibly)
South Korea	-	X	X (possible if Sweetie is not considered a coercive measure)
Spain	-	X	-
Turkey	-	X	-
USA	-	X	X

4.8.4 Reasonable suspicion

The previous subsection showed that in about half of the investigated jurisdictions, as of the writing of this report, the chatbot cannot be employed because there is an insufficient legal basis. Furthermore, as discussed in the chapter on substantive criminal law, the use of Sweetie may be blocked because having a sexually charged interaction with a virtual minor is not considered criminal. For the latter category, a rationale for using Sweetie nonetheless could be that interacting with Sweetie may give law enforcement reasonable suspicion/ probable cause that someone is guilty of a(nother) crime, enabling law enforcement to employ other investigative techniques, such as searching a suspects' home.

In these instances, the gathered evidence cannot be used to prosecute the suspect for crimes against a digital character, but the information could yield a reasonable suspicion or probable cause that the person in question may have committed another relevant crime, be it webcam-facilitated abuse of real children, or the possession, creation, or accessing of child pornography.

[196] As indicated above Israel's practice is not based on case-law or statutory laws, but on the exercise of unwritten powers.
[197] This interpretation of the Polish Police Act still has to be confirmed by the courts.

If the chat, for instance, clearly shows that the person has experience in discussing webcam sex with children, then that might be sufficient for assuming he has likely committed a webcam sex crime before. In a similar vein, if the person sends to the avatar child pornographic material in order to corrupt or groom it, this would be a strong indication that the suspect is indeed in possession of such material. These indications would then trigger investigation procedures coupled with the prevention/ investigation of sexual crimes against real minors, which would be guided by the already existing and regulated investigation means.

For the legality of the above approach, the use of Sweetie must be allowed in some shape or form in domestic criminal procedure law. Furthermore, the possibility of taking this road will inevitably depend on the particularities of the criminal system, and on the interpretation of the standards of reasonable suspicion[198] and probable cause[199], which is a 'value judgement'[200]. In Turkey, for instance, an official investigation can already be triggered by 'simple suspicion',[201] while coercive powers such as search or seizure of computer devices can only be set in motion upon 'strong grounds of suspicion'[202]. The Nigerian Penal Code in its turn speaks of 'reasonable grounds' when it comes to authorising intrusive investigation procedures in relation to serious crimes.[203] We found similar formulations in most of the investigated jurisdictions.

However, it is beyond the scope of this report to discuss the exact scope of these standards and how they would apply to information obtained through the use of Sweetie. At this point it suffices to have drawn the reader's attention to the matter.

4.9 Summary and conclusions

Based on the legislation and case law discussed above, we conclude that there are still serious legal impediments to (widely) employ the methodology of Sweetie in about half of the studied countries (see Table 7 above). This is mainly due to the absence of a clear legal basis.

The necessity for a specific legal basis stems directly from Sweetie's intrusive nature as an investigation tool that interferes with fundamental rights. However, we found that none of the jurisdictions at hand has enacted legislation that would explicitly consider artificial intelligence software systems as a means of investigation. Some jurisdictions compensate this lack of provisions with the analogous or direct application of other investigatory powers, while in other jurisdictions the existing investigatory powers appear insufficient to allow such an approach.

The inability to use existing investigative powers has in large parts to do with Sweetie's hybrid nature, combining a variety of investigatory methods that interfere with privacy (by

[198] In the US, for instance, reasonable suspicion is considered less than probable cause both in quality and quantity, but courts have failed to provide further guidelines. See Alabama v White, 496 U.S. 325, 330–31 (1990).
[199] Probable cause is considered by some an 'articulable belief that a search will more likely than not *produce* significant evidence of wrongdoing', see Slobogin, C 2012, 'Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory', pp. 12-22.
[200] Taslitz, AE 2013, 'Cybersurveillance without Restraint: The Meaning and Social Value of the Probable Cause and Reasonable Suspicion Standards in Governmental Access to Third-Party Electronic Records', p. 887.
[201] See country report on Turkey, p. 19.
[202] See Art. 134 of the Turkish Criminal Procedure Law.
[203] See Country report on Nigeria.

intercepting communications and recording them) and fair trial rights (considering its capacity to actively participate in said communications by interacting with suspects and potentially entrapping them). In several countries, the investigated jurisdictions have legislation in place to authorise the first conduct, but not the second, and are therefore incapable of comprehensively implementing Sweetie. This is the case in Argentina, Brazil, Israel, Spain and Turkey. These countries would have to enact particular legislation to fulfil the criteria laid down in international and national legislation on fundamental rights. On the one hand, these countries do not criminalise the (attempted) abuse of virtual characters, and therefore the conduct does not warrant use of investigation powers. On the other, undercover operations are either not covered by the law at all, or only with regard to a short list of offences, excluding crimes against the sexual integrity or other offences that could be potentially relevant in the context of webcam child sex tourism. It remains to be seen whether these insufficiencies can be circumvented by interpreting the information delivered by Sweetie as a reasonable suspicion/ probable cause to authorise investigative measures.

As for the rest of the studied countries, Sweetie's application in investigations is likely to fit the legality standards only in regard to the coercive powers authorising it in the first place. While said application scope seems rather limited in Belgium, the Philippines and Poland, which focus on particular online offences, the chatbot and its features appear to satisfy the constitutional requirements in Australia, Canada, Croatia and England and Wales. These countries have developed substantive and procedural means to tackle the online abuse of children. Especially, the enactment of laws against the online grooming of children has prompted a perceivable shift in the investigation techniques as well, allowing for more proactive policing of online communications and for applying existing tenets on entrapment techniques to undercover investigations when targeting an area and not a particular suspect.

5 Digital Forensics

Undercover operations that would use Sweetie to apprehend webcam child sex offenders require not only a legal framework that authorises such an investigation tool. As the chatbot is primarily intended to facilitate the identification of perpetrators, it brings about questions on the evidentiary rules applicable to the collection of evidence from the chat communications and webcam streams. Therefore, in the following subsections we elaborate upon the general requirements applicable to (digital) evidence and how the countries in this study implement these.

5.1 Generally accepted standards

Criminal investigations aim to follow the trail that offenders leave while committing the crime and to link suspects to the crime.[204] The information gathered with this purpose, i.e. the evidence of the crime, has to be preserved and examined in a particular manner to maintain the objectivity called for by the investigative process,[205] and to be introduced in court accordingly. While this is a general tenet from traditional forensic disciplines, it applies to online investigations and digital evidence as well, and means that the cyber-trail is to be rigorously followed. In this regard, progress has been made by law enforcement in the digital evidence gathering, be it by furthering the expertise of police officers in handling technology or by involving IT experts who oversee or perform the information gathering themselves. By now, courts are also used to dealing with digital evidence and deem it admissible, provided that its authenticity and integrity are ensured.

5.1.1 Authentication and chain of custody

The authentication of evidence ensures that the obtained information is the same as the originally seized. One of its most important objectives is maintaining and recording the chain of custody, which requires that each person who handles the evidence including the handling itself must be documented, and may be summoned to testify on the originality of the evidence in court.[206] An improper chain of custody may result in the contamination or loss of evidence. The chain of custody requirements apply likewise in the context of digital evidence.

5.1.2 Evidence integrity and digital fingerprints

Integrity checks further support the authentication process by ensuring that the evidence has not been altered since the time of its collection. In digital forensics, this is usually done by a comparison of the digital fingerprint of the evidence at the time of collection with the digital fingerprint of the evidence in its current state.[207]

5.2 Implementation of digital forensics in the compared jurisdictions

When dealing with the standards of digital forensics, we observed that all of the jurisdictions at hand admit electronic evidence in court. While some, following specific incentives introduced by the Cybercrime Convention, have already enacted particular legislation, others

[204] Casey, E 2011 'Foundations of Digital Forensics' in E Casey (ed), *Digital Evidence and Computer Crime*, p. 16.
[205] Casey, E 2011 'Foundations of Digital Forensics' in E Casey (ed), p. 19.
[206] Casey, E 2011 'Foundations of Digital Forensics' in E Casey (ed), p. 21.
[207] Casey, E 2011 'Foundations of Digital Forensics' in E Casey (ed), p. 22.

still lack provisions on the technical requirements and expertise that need to be met when gathering digital evidence.[208] In the case of the latter, the law deals with electronic evidence in the same way as with any other type of evidence. Although this means that the general rules on the authentication and integrity of evidence are observed, the fact that no formal technological standards exist may compromise the gathered information.

Many have adopted diverging approaches. In Australia, evidence from electronic sources is routinely adduced through the questioning of qualified expert witnesses, such as the particular analyst who conducted the forensic examination.[209] Also in the Polish law enforcement practice, the expert witness report would likely be the piece of key evidence.[210] In Estonia, the role of the expert witness is prescribed by the Forensic Examination Act, which states that 'information technology examinations' regarding materials in relation to the sexual abuse of minors should be performed by the Estonian Forensic Science Institute'.[211]

Yet other countries foresee a more active role of law enforcement officers in the handling of digital evidence and supplement their functions with additional technological tools. In Spain, while expert opinions will still be indispensable to identify the true origin of a communication[212] in a troublesome case, Art. 588ter f) of the Criminal Procedure Act ensures the integrity of the digital information by introducing electronic signatures that affirm the origin and destination of the communication.[213] Similarly, shortly after the introduction of electronic signatures[214] by Provisional Measure (MP) 2.200/ 2001[215], the Brazilian legal system has adopted notarial minutes[216] as a supportive evidential standard. While said minutes are regulated under the Code of Civil Procedure, the criminal system recognizes them as appropriate for the purpose of criminal proceedings.[217] Put together with electronic files or digital documents, the notarial minutes support the credibility of any content taken from the web. However, notarial minutes apply to publicly available content only.

In the US, when it comes to online chat conversations officers are generally encouraged to use a screenshot or a browser's saving function to limit their interference with the content.[218]

---

[208] This is true for Belgium (see country report on Belgium, p. 44), Canada (country report, p. 53), Croatia (country report, p. 34), Israel (country report, p. 16), Nigeria (see country report, p. 50), the Philippines (country report, p.37), and Scotland (country report, p. 21).
[209] See country report on Australia, p. 26.
[210] See country report on Poland, p. 36.
[211] Regulation on the list of examinations conducted in EFSI, subsection 5(3)(1). Available from: https://www.riigiteataja.ee/akt/13365049. [28 September 2016].
[212] Judgement of the Supreme Court of Justice 300/2015 delivered on 19 May.
[213] Spanish report, p. 40.
[214] This is a digital certificate issued by the Brazilian Public Infrastructure Key (ICP-Brazil), which awards electronic files a presumption of veracity. For more on the matter see country report on Brazil, p. 24.
[215] In the Brazilian legal system provisional measures have a temporary validity and are issued by the President of the Republic in urgent situations. See https://www.oas.org/juridico/mla/en/bra/en_bra-int-des-ordrjur.html. Provisional Measure (MP) 2.200/ 2001 is available at http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm. [14 September 2016].
[216] Regulated in Article 384 of the CPC. Notarial minutes enhance the credibility of images, audios, videos and writings taken from web pages that could have been easily amended or deleted.
[217] See Brazilian report, p. 27.
[218] See United States v Jackson, 488 F. Supp. 2d 866 (D. Neb. 2007).

5.3 Storing data from online chats and chatroom activity

Given that webcam streams, unlike downloads, are not by default stored on the personal computer of the victim or the suspect, the criminal systems that lack provisions concerning content interception of online communications may experience practical issues to prove illegal webcam sex, as witness statements or seized electronic devices may not be available.

However, it is possible to gather other forms of evidence related to the webcam streams, such as for instance chat logs that have been saved. When Sweetie is used by law enforcement, then streams can also be recorded. Investigation agents can further take screenshots, when deemed necessary. Such records would be crucial to make the evidence available in court.

In addition, the chat scripts of the avatar should also be added to the other relevant information for the consideration of the judges before sentencing. This way the court would be able to gain an insight into how the avatar has approached the communication and whether any impropriety could be witnessed on the part of the AI agent, for instance, whether it complied with the 'essentially passive' standard required to avoid entrapment.

5.4 Summary and conclusion

While the investigated jurisdictions do follow the generally accepted forensic standards such as observing the chain of custody and taking precautions to maintain the integrity of the evidence, only some of them have taken particular steps towards the implementation of digital forensics agendas. Therefore, the available lessons from the practice vary and law enforcement agencies (would likely) approach the collection of evidence from chat communications and webcam streams differently. The lack of uniformity bears risks for the comprehensiveness of future investigations of webcam crimes (against minors), and may present challenges for the handling of the gathered information and for its sharing in trans-border operations.

6 Jurisdictional concerns with the application of Sweetie

As indicated in chapter 3,[219] depending on the exact conduct of the suspect and how he would approach Sweetie during the chat conversation, there are some avenues for prosecuting him for soliciting (or attempting to have) webcam sex. However, as webcam child sex tourism crosses national borders and implies scenarios in which, as a rule, victim and offender reside in different countries, jurisdictional conflicts inevitably present themselves.

The latter can be best illustrated by means of the following example. Let us assume for the sake of the study that UK law enforcement authorities use Sweetie to conduct a luring operation in a public chatroom for users under 18 years. Through Sweetie's solicitation by suspects and its communication with the latter, they manage to collect enough information such as IP addresses and Skype handles to identify a number of individuals, some of which reside in Australia and Spain. The computer devices of those alleged offenders and (parts of) the potential evidence of their interactions with Sweetie would be stored beyond the physical reach of the UK officials, which means the latter will have to resort to remote transnational information searches. In so doing they would primarily face two legal difficulties: what legal grounds would entitle them to start an investigation, and under what circumstances can the investigation be conducted (also abroad)?

The first question is closely connected to the states' jurisdictional capacity to prescribe rules, but also with our finding that the different actions of the offender in front of the webcam or as a part of a chat conversation with Sweetie trigger different norms under domestic law. The second issue on how to enforce investigative procedures in relation to offences against Sweetie has to do both with the available coercive powers discussed in chapter 4, and with the general jurisdictional tenets on enforcing state laws. Therefore, to answer these questions and explain what the likely outcome of our example would be in practice, in the following sections we apply the international law rules on state jurisdiction to trans-border cyber-investigations, and subsequently to the case of Sweetie.

6.1 Grounds for the exercise of jurisdiction in cybercrime investigations

Across frontiers, powers are differently distributed and restricted, and it is international law that governs the legal framework of interaction. Thus, it comes as no surprise that the state's operation of coercive powers abroad is subject to strict international limitations. Said operational limitations are inherent in the rules of state sovereignty, which in their turn have effected a differentiation between a state's power to regulate or otherwise impact people, property and circumstances[220] (usually referred to as prescriptive jurisdiction), and its ability to enforce it (enforcement jurisdiction).

Both these competences, although originating from the same notion, have an impact of their own in the criminal context at hand, and are conditioned upon a certain link to the state willing to assert them.

[219] See table 4: Criminalisation of (attempted) webcam sex with Sweetie.
[220] Shaw, MN 2014, *International Law*, p. 469.

6.1.1 Prescriptive jurisdiction

States' jurisdictional claim to prescribe law can be premised on a number of factors.[221] The state's direct proximity to the crime scene has enhanced the traditional idea that a crime is best punished locally.[222] The principle of territoriality is, therefore, one of the main grounds for the exercise of criminal jurisdiction, and gives states the right to exercise it regardless of the offender's nationality.[223] However, the territoriality principle is more comprehensive than one assumes it to be at first glance, as it applies also to crimes committed only partially on the territory of a state.[224] This is the case where, for instance, the criminal conduct has been initiated in one state, but completed in another.[225] Under such circumstances, both states would have criminal jurisdiction to try the perpetrator – the first under the principle of subjective territoriality, the second one under the objective territoriality principle.

Further, the principle of nationality, the state's special link to its population, allows a state to domestically regulate the conduct of its nationals wherever they are. Therefore, states are also entitled to claim jurisdiction over offences committed by their nationals abroad,[226] and can do so even if the suspect has a dual nationality.[227] Often, countries opt for additional statutes that regulate precisely which offences trigger jurisdiction over nationals abroad.[228]

In addition, a state can seek to regulate conduct under the passive personality principle and the protective principle.[229] The former, a disputed practice, allows states to exercise jurisdiction over anyone who harms their nationals. The latter justifies regulating conduct that produces harmful effects within a state's territory and thus endangers national (security or economic) interests. The 'effects' theory is widely accepted in the international community and often used in treaties.[230]

Since technology-specific rules on state jurisdiction do not exist, the exercise of jurisdiction over cybercrimes remains largely based on the approaches outlined above, among which the principle of territoriality plays the most pivotal role. Although this may appear odd when dealing with criminal behaviour portrayed in the 'de-territorialised'[231] space of the Internet, international law so far has imposed very few limitations on states when they claim criminal jurisdiction over cybercrimes, and relies on their willingness to resolve positive jurisdictional clashes by rather informal means.

---

[221] Shaw, MN 2014, *International Law*, p. 474; Klabbers, J 2013, *International Law*, p. 91.
[222] August, R 2002, 'International Cyber-Jurisdiction: A Comparative Analysis', p. 534.
[223] Gillespie, AA 2012, 'Jurisdictional issues concerning online child pornography', p. 153.
[224] Shaw, MN 2014, *International Law*, p. 475.
[225] The classical example explaining such a situation is where a person shoots at someone across a border and kills them in the neighbouring state.
[226] Shaw, MN 2014, *International Law*, pp. 479 ff.
[227] Harris, D 2010, *Cases and Materials on International Law*, p. 230.
[228] This is often the case in common law countries. See on this issue Shaw, MN 2014, *International Law*, p. 481.
[229] A further possible base for the assertion of state jurisdiction – the universality principle – will not be discussed here. Although webcam sex crimes against children are a highly serious matter, they do not form part of the group of war crimes and crimes against peace or humanity that trigger universal jurisdiction due to the particular danger their represent for the international community as a whole. See on this Shaw, MN 2014, *International Law*, pp. 485ff.
[230] See for instance the 1979 Hostages Convention, the Aircraft Hijacking Conventions and the 1994 Safety of UN and Associated Personnel Convention.
[231] Ryngaert, C 2015, *Jurisdiction in International Law*, section 3.5.

6.1.2 Jurisdiction to enforce

Enforcement jurisdiction is another matter. Although a state may have jurisdiction to prescribe rules that even portray a certain extraterritorial reach, it generally cannot enforce said laws (whether by judicial or executive organs) outside its territory without the affected state's consent. As states are independent from each other and possess territorial sovereignty, the capacity of a state to operate within the borders of another state is essentially restricted by the sovereign powers of the latter. Translating this into the criminal context means that although a state may claim criminal jurisdiction based on rules enacted according to its prescriptive jurisdiction, law enforcement usually sees itself constrained to finding evidence and apprehending the alleged offender within their own territory, or acquiring these from other states' territory through mutual legal assistance.

6.1.2.1 Extra-territorial application of investigative power

The observations made above mean that trans-border investigations are not allowed unless expressly consented by the host state[232] or established by an international agreement. The same applies to investigative techniques conducted in cyberspace such as remote information searches that aim, for instance, at accessing and securing information from a server located abroad. Opposing opinions that advocate a different understanding when investigators do not physically enter the other state's territory[233] are not tenable under the current state of international law. While admittedly this is not so much a question of substantively threatening the territorial integrity of the state hosting the data, such practices interfere with the state's sovereign control over its citizens and their rights as it subjects them to foreign legislation and law enforcement. The state sovereignty breach may therefore easily result in a breach of the laws on criminal procedure and the corresponding procedural guarantees.

Therefore, in the event of unauthorised remote investigations, some of the countries studied for the purposes of this report render criminal procedures against a national inadmissible if the procedure has been based on evidence obtained by entrapping the suspect, or the use of other coercive techniques by foreign police agents.[234] However, in some of the criminal systems such information may also be considered a reasonable suspicion that triggers investigative procedures on the national level.[235]

Yet some other criminal systems at hand are willing to take into account evidence that has been brought about by the investigative powers of foreign agencies that may have trespassed their enforcement powers and thus violated the territorial sovereignty of other states. In the Netherlands for instance, the *Schutznorm* principle allows the use of such evidential material if Dutch authorities have not been involved in acquiring the data.[236] A further interpretation of

[232] Shaw, MN 2014, *International Law,* p. 473.
[233] Johnson, DR and Post, D 1996, 'Law and borders: The rise of law in cyberspace', pp.1367-1402; See also United States v Gorshkov, No CR00-500C (W D Wash May 23, 2001), where the US claimed that they did not violate Russian sovereignty because the FBI agents never left US soil.
[234] That is the case to a certain extent in Belgium. See Belgian report, p. 35.
[235] This is for instance the case in Argentina, see country report on Argentina, p. 27.
[236] Rb. Alkmaar 19 February 2004, LJNA05509, case no. 14.060137-02, to be found at http://www.rechtspraak.nl; Rb. Groningen 16 October 2003, LJNAM1882, case no. 18/076010-01, published in 2003 *Vakstudienieuws,* 56.4 and at http://www.rechtspraak.nl. See also Hock, AA and Luchtman, MJ 2005, 'Transnational cooperation in

the same principle allows for the use of the evidential information if the foreign agency ends up obtaining the information on the individual without actually targeting him, but its own nationals.[237]

In any event, the exercise of investigative powers outside of national borders and its consequences would depend on the jurisdiction(s) involved and the case in question. For the purposes of this study it suffices to have highlighted that it interferes with the targeted state's sovereign competence to govern its population, and with individuals' privacy and *due process* rights.

6.1.2.2 Mutual legal assistance

States typically address the gap between their capacity to regulate and to enforce by relying on mechanisms for legal assistance, which are usually referred to as treaties on mutual legal assistance or MLATs. There are countless multilateral and bilateral agreements between states that establish procedures for obtaining and providing assistance in transnational criminal matters.[238] Normally, a request for assistance, for instance, to locate or to arrest a person, to produce documents or records, or to perform a search, can only be denied on the grounds specified in the respective treaty.

Further, it is important to note that MLATs are rather context-specific or offence-specific, and may therefore never cover the entire range of circumstances leading to a particular investigation. That is to say, if the requested procedure or coercive power is not explicitly covered by an agreement, a request for assistance will be (formally) devoid of any prospects from the very beginning. The same applies if the alleged criminal conduct is not listed in the agreement. Any further steps of the investigation would then lie with the good will of the agencies across the border.

Where MLATs do not exist the investigation authorities employ informal means of cooperation. These tend to be even more difficult to use, as they may involve multiple states with varying legal systems, and therefore different understandings as of what constitutes a criminal offence. If one of the states involved has not criminalised the alleged conduct under its national law, the requirement of double criminality[239] cannot be fulfilled. Said state will likely have no interest in contributing to the investigation.

6.2 Translating the jurisdictional rules to the context of Sweetie

Let us now apply the jurisdictional tenets described in the preceding sections to the case of Sweetie. Since prescriptive jurisdiction can be claimed on a number of grounds, it means that

---

criminal matters and the safeguarding of human rights', p. 4. The Israeli system also suggests that evidence against nationals obtained by foreign agents in an unauthorized trans-border operation would be admissible.

[237] Ibid at fn. 209.

[238] Bellia, PL 2001, 'Chasing bits across borders' in *University of Chicago Legal Forum*, p. 50. See for instance Commonwealth of Independent States Agreement, Art. 5; Council of Europe Cybercrime Convention, Art. 23; Shanghai Cooperation Organization Agreement, Art. 3-5. Art. 28 (2) of the AU Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV), Malabo, 27th June 2014.

[239] The principle of double criminality was introduced by extradition treaties and requires the act to which a request relates to be a crime under both the criminal law of the requested state and the requesting state. For a comprehensive discussion on this see Williams, SA 1991, 'The Double Criminality Rule and Extradition: A Comparative Analysis', p. 582.

also in our example several states will be able to do so over crimes against Sweetie, as the Internet amplifies the existing options. The initial act's location (presently Australia or Spain, from where the alleged child offenders have accessed the chatroom) or where it has its effect (Sweetie's location), as well as the location of the chatroom servers or other hardware (which may be in any country around the globe) can establish a sufficient link to a country to claim jurisdiction; there are states that even use the location of anything remotely connected to the crime to claim jurisdiction.[240] Thus, although it is the UK that has initiated the investigation in question, it may be difficult to establish who has the stronger jurisdictional claim.

The enforcement side of the question brings about additional challenges. As remote information searches are 'not distinguishable in legally relevant ways'[241] from physical searches, directly pursuing the digital trail of the webcam offenders would mean to engage with the territorial sovereignty of Australia or Spain, or any other state that could potentially harbour (parts of) the searched data. Consequently, in order to obtain computer data physically located on Australian or Spanish territory, UK's law enforcement must either obtain the consent of the state authorities to continue the search or resort to traditional procedures of mutual legal assistance.

6.2.1 Mutual Legal Assistance in the case of Sweetie

UK law enforcement may be able to resort to an existing MLAT on cybercrime. Surveys, however, show that cybercrime MLATs tend to focus on matters of extradition rather than on evidentiary procedures.[242] Thus, there is a chance the requested investigative act would not be explicitly covered by the respective treaty, which as explained above would lead law enforcement to resort to informal means of cooperation.

In the context of webcam child sex tourism the lack of a concrete MLAT is not unproblematic, since, as described in the third chapter of this study[243], states tend to criminalise webcam sexual abuse through different legal constructions. While the offender's conduct in the UK may fall under the offence of attempted child prostitution, the same conduct against Sweetie would fall in Australia under the crime description of attempted sexual abuse or grooming, whereas in Spain an inappropriate interaction with Sweetie would not be criminal at all. This would hinder the establishment of double criminality, which is essential for triggering investigative procedures abroad.

In addition, electronic evidence may simply be lost after a short period of time. This is critical considering the fact that legal assistance mechanisms require time to be set in motion. The time needed to issue a request and to eventually execute it on the other side of the border usually costs the authorities their opportunity to secure volatile electronic evidence.[244] In the case at hand this consideration is of particular importance given that webcam streams produce mainly volatile data that can be lost completely once the suspect has powered down his computer.

[240] See, for instance, the cybercrime jurisdiction provision of Malaysia, Art. 9 Malaysia Computer Crimes Act 1997. More on that in Brenner, SW & Koops, BJ 2004, 'Approaches to Cybercrime Jurisdiction', pp. 21-23.
[241] Bellia, PL 2001, 'Chasing bits across borders' in *University of Chicago Legal Forum*, p. 62.
[242] United Nations Office on Drugs and Crime 2013, *Comprehensive Study on Cybercrime*, p. 200.
[243] Compare table 4: Criminalisation of (attempted) webcam sex with Sweetie.
[244] Current reports indicate that responding to a request can actually be a matter of months. For more on this: United Nations Office on Drugs and Crime 2013, *Comprehensive study on cybercrime*, pp. 197ff.

6.2.2 The Cybercrime Convention

Against the background of the challenges of standard MLATs and their potential interplay with Sweetie's case outlined above, a legal instrument that deserves our attention is the Cybercrime Convention. This tackles some of the shortcomings that result from out-dated and lengthy MLA procedures.

The Convention establishes mandatory contact points (24/7 networks) between national agencies, which are meant to ensure the immediate assistance in investigation matters.[245] The treaty further addresses consent and procedural difficulties between national agencies by streamlining investigation procedures and defining four methods for securing computer data, namely expedited preservation of stored computer data, expedited disclosure of preserved traffic data, real time collection of traffic data, and interception of content data.[246] In this context, signatory parties are obliged to confer said competences to their national authorities so the latter can both obtain and request the disclosure of data. However, the Convention, which can also be acceded by non-Council of Europe states and has therefore gained in importance globally, leaves jurisdictional clashes unresolved, as it does not provide guidance, or sets up mechanisms, for prioritising competing jurisdiction claims.[247]

Moreover, although this approach and the procedures it introduces clearly go far beyond ordinary mutual assistance mechanisms,[248] they are still confined within the borders of the state where the data is physically located. The Convention thus does not bring about new approaches for dealing with *trans-border* investigations, but largely relies on traditionally known and well-recognised jurisdictional concepts. The power to search, seize, or intercept digital evidence remains in the hands of the host state, and transnational investigations are not welcomed under the Convention's provisions.[249] The only exception is article 32, which allows cross-border access to publicly available data (which is not very relevant in the case of Sweetie, except perhaps for securing data from publicly accessible chatrooms),[250] as well as cross-border access to data with voluntary consent from someone who has the lawful authority to consent.[251] That will usually be the foreign state, although it may also include service providers (e.g., chatroom providers) if data protection and contract law allow them to consent to law enforcement accessing the data at issue (which is unlikely to be the case in our example). Efforts to draft an additional protocol to the Convention on trans-border access to data have not been successful and seem on hold at the moment; it will likely take a long time before countries will be ready to agree on some international agreement on trans-border access to data.[252]

---

[245] See Art. 35 CCC.
[246] Council of Europe Cybercrime Convention, Arts. 29-31, 34.
[247] See Art. 22 (5) CCC. The provision merely stipulates that states should be the one to determine 'the most appropriate jurisdiction for prosecution', but a further elaboration upon this 'appropriateness test' is missing.
[248] Bellia, PL 2001, 'Chasing bits across borders' in *University of Chicago Legal Forum*, p. 59.
[249] The Convention's provisions stipulate clearly that the respective procedural rules are applicable only within a state's territory. See Art. 18, 19, 20, 21 CCC, which explicitly refer to national territory.
[250] See Art. 32 (a) CCC.
[251] See Art. 32 (b) CCC.
[252] See, extensively, Koops, BJ and Goodwin, M 2014, *Cyberspace, the cloud, and cross-border investigation: The limits of international law*.

Thus, although all three countries from our example have signed and ratified the Convention, the UK law enforcement officials have to reach out to their counterparts in Australia and Spain to formally request the securing of the data needed for an investigation of an offence against Sweetie.

6.3 Conclusion

By highlighting the existing tension between, on the one hand, a global communications network where webcam child sex tourism can take place across borders, and, on the other, law enforcement procedures that remain tightly restricted to national territory, this chapter has called attention to the problematic nature of the enforcement of criminal law. Law enforcement, but more relevantly regulators and policy-makers, should be aware of the jurisdictional challenges in the context of Sweetie. We conclude that as states and their law enforcement agencies continue to move within a consent-based legal framework, a more effective way of cross-border investigation is necessary. In the case of Sweetie, the lack of international harmonisation makes itself especially felt, because of the divergence of criminal provisions and instruments,[253] which affect the scope of and possibilities for international cooperation.

With regard to webcam child sex offenders, law enforcement agents will have to rely on the willingness and expedited proceedings on the part of their foreign colleagues when further investigating a suspect's digital trail. Be it following the Cybercrime Convention's standards or MLAT procedures, when it comes to securing digital evidence,[254] the agent's law enforcement powers end at their respective national borders. As with other forms of cybercrime, this fact may significantly undermine the effectiveness of investigations against suspects using Sweetie.

[253] United Nations Office on Drugs and Crime 2013, *Comprehensive study on cybercrime*, p. 208.
[254] Koops, BJ and Goodwin, M 2014, *Cyberspace, the cloud, and cross-border investigation: The limits of international law*, p. 14.

7 Effective and legitimate use of Sweetie: the way forward

In the following we discuss the main substantive, procedural and jurisdictional issues in Sweetie's implementation identified in the present report, and possible ways to address these.

7.1 Legal uncertainties and restrictions for the use of Sweetie

7.1.1 Substantive law restrictions

Based on our research we have identified several issues that need to be remedied in order to effectively and legitimately combat webcam sex using Sweetie. This would in most cases entail changes to substantive criminal law. Whether or not countries want to actually adapt their substantive criminal law in order to facilitate the use of Sweetie is a question of a political nature.

1) Clarifying substantive law

In most jurisdictions under examination we see that webcam sex with minors is criminalised in one form or another. However, given that in most jurisdictions this relatively new form of crime is 'read' into existing crime descriptions there are questions regarding the extent to which this behaviour is criminalised.

In order to avoid stretched legal interpretations that might be at odds with the principles of legality and legal certainty, it is recommended that legislators include in their crime catalogues (more) explicit definitions of ambiguous terms such as 'pornographic' and 'sexual activity/ abuse' and more guidance on what kinds of behaviours associated with webcam sex fall within which crime descriptions.

Changing substantive criminal law in order to facilitate the use of Sweetie

Sweetie is first and foremost an innovative investigation tool. Its innovativeness entails that in order for it to be used legitimately, changes to substantial criminal law will most likely need to be made. As it stands, several jurisdictions may not deem interacting with Sweetie in a sexually charged way a criminal offence at all. In these jurisdictions it will be hard to justify the application of Sweetie by law enforcement, because the behaviour Sweetie elicits and exposes is actually not criminal at all.

If these jurisdictions wish to allow the use of Sweetie by law enforcement, it stands to reason that they change their substantive criminal law systems in such a way that the intention of the suspect is the determining factor in establishing criminal liability. This will mean a shift from an 'act based' criminal law system towards a more 'intention based' criminal law system. Whether combating child sex abuse using Sweetie necessitates such a shift in the approach to criminal law is a matter of ethics and politics.

Jurisdictions that already criminalise virtual child pornography and/or the grooming of virtual characters, or those considering criminalising these acts (such as for instance the Netherlands in the case of grooming), should also consider including subjective elements in provisions that relate to child (webcam) sex abuse. An inconsistency in the approach to criminalisation of child

(webcam) sex abuse may create normative gaps, so from a legal-systematic viewpoint it makes sense to extend criminal liability to related offences.

International harmonisation
Last, but not least, it is recommended to discuss a global approach to dealing with child webcam sex tourism using tools such as Sweetie, in order to avoid crime and penalty havens and to create more legal certainty. If consensus is reached, this must be reflected in international legal instruments such as the Lanzarote Convention and the OPSC. International investigations and mutual legal assistance procedures would benefit from domestic systems that criminalise webcam child sex exploitation in similar terms and through similar crime descriptions.

7.1.2 Procedural law restrictions

In terms of criminal procedure, we have found that the jurisdictions at hand have all introduced coercive investigative powers to address serious and organised crime. While a fair number of these investigative powers may also be applied in an online context, most of them are still 'traditional'. That is to say, they were written in large parts for the 'offline world' and do not readily accommodate the use of innovative investigative tools such as Sweetie.

A particular issue when it comes to the application of Sweetie is its 'hybrid' nature as a lure, an apparatus for recording conversations and video and an intelligent undercover agent. If law enforcement wants to use Sweetie, it is important to determine whether existing investigative powers used either alone or in conjunction, cover the application of Sweetie. Given the possible infringement of privacy, both in cases where the use of Sweetie is covered by existing investigative powers and in cases where new legislation is introduced, the application of Sweetie must be in accordance with the law. That is to say the laws governing the use of Sweetie must be accessible and of sufficient quality.

With regards to the issue of entrapment, it is relevant that the application of Sweetie follows existing guidelines on targeted and non-targeted entrapment. Law enforcement should carefully consider in which chatrooms Sweetie is placed and how she will interact with suspects via her chat script. Particular attention needs to be devoted to the hybrid character of Sweetie as a lure and as an undercover agent. In more traditional settings these investigative functions are not combined. In this sense the existing use of human lures (e.g. law enforcement officers posing as minors in a chatroom) is instructive.

If the use of Sweetie necessitates changes to criminal procedure law, it is also relevant to include explicit standards in the handling of digital evidence.

7.1.3 Adressing jurisdictional constraints

A way to possibly avoid more complex jurisdictional questions and competing jurisdictional claims (as outlined in the preceding chapter) would be to primarily use Sweetie to investigate nationals or residents of the respective country. This can be done by focusing on local chatrooms (intended for and frequented by national users), which would lessen the difficulties of obtaining the necessary authorization for using coercive powers, and of physically securing and investigating the devices used by offenders if needed. This task could be further facilitated

if following the examples set by Australia, Canada and the UK on the matter, states legislate the criminality of a country's citizens' committing crimes against children extra-territorially.

A possible way to facilitate cooperation and to alleviate jurisdictional conflicts in relation to trans-border investigations of webcam child sex tourism and other child exploitation offences would be to adopt an Optional Protocol (OP) to the Lanzarote Convention on the matter.

OPs have the advantage of introducing additional provisions, procedures and mechanisms to the original treaty by maintaining the latter's scope and integrity. Human rights treaties for instance, oftentimes provide in their OPs for complaint procedures that address alleged human rights abuses, or regulate substantive law areas not considered previously. States have no obligation to ratify those protocols, but can do so if they think that said instruments enhance their national interests or broader policy and international cooperation agendas.

An OP to the Lanzarote convention that regulates cross-border investigations would have following advantages:

- It could provide guidance on how to deal with positive jurisdictional conflicts in relation to trans-border investigations of (Internet) child sex/ abuse offences only, thereby avoiding broader commitments which are not likely to be accepted by sovereign states;

- The OP would bindingly stipulate the forensic standards required for handling data searches and the resulting evidence, prompting states that have not yet introduced digital agendas to do so, and preventing the loss of digital evidence due to improper handling.

8 Summary and conclusion

Webcam sex tourism, the act of engaging children in webcam prostitution, is a growing international problem. Not only does webcam sex tourism provide easy access to child abuse and child abuse images for child abusers, it also a crime that has a comparatively low risk for the offenders. Live webcam performances leave few traces and little evidence that law enforcement can use. Further difficulties arise from the fact that webcam sex tourism often has a cross-border character, which causes jurisdictional conflicts and makes it more difficult to obtain evidence or even launch an investigation.

The Dutch children's rights organization Terre des Hommes (TdH) was the first NGO to actively tackle webcam child sex tourism by using a virtual character called 'Sweetie' to identify offenders in chatrooms and online forums. An agent of the organisation operated the Sweetie avatar, posing as a ten-year old Filipino girl, in order to gather information on individuals who contacted Sweetie and solicited webcam sex. The gathered information was subsequently handed over to the authorities, who thereupon were able to launch investigations in various countries.[255]

One of the major drawbacks of Sweetie 1.0 (and law enforcement in general) is that the avatar could not be deployed at scale. Human operators can only engage in a limited number of conversations with suspects, while the (potential) solicitations addressed at Sweetie 1.0 far exceed that number. Sweetie 2.0 aims to solve this problem. Sweetie 2.0, being an artificial intelligence, is far more scalable because multiple instances of Sweetie can be deployed simultaneously.

But using an artificial intelligence like Sweetie raises serious legal questions. Sweetie as an investigative tool is so innovative, that it is unclear whether its use is actually covered by the existing rules of criminal procedure. However, the question of criminal procedural legality of Sweetie is preceded by a prior substantive criminal law question: is interacting with Sweetie in a sexually charged way a criminal offence in the first place, given that Sweetie is not a person, but a virtual avatar? An answer to this question is important, because if webcam sex tourism with a virtual avatar is not considered criminal, it will be much harder to make the case that Sweetie is an acceptable investigative method.

We will discuss the substantive criminal law issues and the criminal procedure law issues separately below.

8.1 Substantive criminal law issues

In our research we have identified the following issues that impact the application of substantive criminal law:

[255] Further information on the project known as 'Sweetie 1.0' can be found on www.terredeshommes.nl/en/sweetie-face-webcam-child-sex-tourism. [28 September 2016].

1. Sweetie is not an actual person and as such sexually charged interactions with Sweetie may not be considered criminal in jurisdictions criminalising only certain interactions with real persons (e.g. the Netherlands).
2. Sweetie is deliberately programmed not to perform sexual acts or to show sexual organs.

In most of the jurisdictions we examined webcam sex with real minors has been criminalised in one form or another (see table 3), however the same cannot be said for webcam sex with a virtual person such as Sweetie (see table 4).

In some jurisdictions someone can never be convicted for committing or attempting to commit an offence against Sweetie (e.g. Brazil and the Netherlands). In other jurisdictions, criminal liability is only limited to the specific offence of grooming (e.g. Argentina and Belgium), which is in many cases not applicable to Sweetie. For most jurisdictions however, it is quite uncertain given an absence of case law (and even literature) on the matter (e.g. Germany, Israel, Poland).

In most jurisdictions the crime descriptions applicable to webcam sex tourism contain a specific mention of 'a person under the age of X years'. Given the fact that Sweetie is not a real person, this element of the crime can never be proven. Furthermore, because Sweetie is not programmed to undress, perform sexual acts or show sexual organs, many crime descriptions such as those related to sexual performances or child pornography, cannot be fulfilled.

Although the crime descriptions related to webcam sex tourism in most jurisdictions can never be fulfilled, there might be room to qualify the behaviour of the suspect as an attempt. In this regard, the doctrine of the inadequate attempt (legal or factual impossibility) is relevant, as it will determine whether an attempt is punishable or not.

When we speak of a legal impossibility, the behaviour, even if completed never leads to a criminal offence, regardless of the criminal intentions of the suspect. The reason for this is that in these cases the behaviour on display itself is not criminal. This can either be the case because the means are absolutely inadequate (e.g. trying to shoot someone by pointing a banana at them), or because the object at which the act is aimed is absolutely inadequate (e.g. trying to murder a corpse).

With a factual impossibility a suspect's intended behaviour would constitute a crime, but the suspect fails to complete the crime, because of a circumstance unknown or beyond his or her control. In these cases the inadequacy of the means or the object are relative. An example of a relatively inadequate means would be an unloaded pistol used to try and shoot a person. An example of a relatively inadequate object is an empty cash register in which someone puts his hand to grab money. Under normal circumstances this would have resulted in the theft of money, but in this concrete case, the attempt fails. In contrast to a legal impossibility, a factual impossibility is punishable.

In the case of Sweetie, the question is whether we should regard Sweetie as an absolutely inadequate object or a relatively inadequate object. Looking solely at the behaviour in relation

to the crime description, we may argue that Sweetie is an absolutely inadequate object: the crime of webcam sex with a minor can never be completed, because Sweetie is not, nor ever will be a real minor. The fact that Sweetie cannot show sexual organs or display sexual activities, further adds to the argument for an absolutely inadequate object.

However, we can also take a somewhat broader perspective and qualify Sweetie as a relatively inadequate object for the crime of webcam sex with minors. The argument would be that the suspect wants to commit the crime of webcam sex with a minor, but is 'unlucky' and picks Sweetie rather than a real minor. This case is comparable to the example of the cash register: under normal circumstances the crime would have been committed, but due to 'bad luck' on the part of the suspect, there is now a factual impossibility.

There is merit to both arguments and when we look at the jurisdictions we have examined, we see that they take different approaches. For instance, there are jurisdictions (such as the Netherlands), that take an objective approach and look at the actual act and thus lean towards legal impossibility, and systems that take a more subjective approach, attaching more weight to the intention of the suspect, leaning more towards factual impossibility.

In particular, countries that come from a common law tradition seem to take a more subjective approach, either in statutory law itself, or in case law (e.g. Australia, Canada, the UK and the US). In these jurisdictions the subjective element of the crime (i.e. the intention of the suspect) plays a more important role than the objective act. If the suspect is under the (false) impression that he/she is communicating with a minor, this is the determining factor for criminal liability.

So as it stands, approaches to criminalising webcam sex tourism vary throughout the world and in many jurisdictions it is still uncertain whether an attempt at webcam sex tourism can be construed at all. Only in those countries that take the intent of the suspect as the determining factor in criminal liability can Sweetie 2.0 be clearly employed as an investigative tool.

For those countries where it is impossible or substantially uncertain to find a crime description that can be used to criminalise webcam sex tourism with a virtual minor, legislative changes are needed in order to enable the use of Sweetie. The choice to move further away from an 'act-based' criminal law system towards a more 'intention-based' criminal legal system in order to combat webcam sex tourism is of a fundamental nature and would require careful ethical and political deliberation.

Finally, from the perspective of law enforcement it may be worthwhile to explore if Sweetie can be used to investigate the crime of webcam sex with a real person, or related crimes. While the interaction with Sweetie may not be considered criminal in itself, it could provide a reasonable suspicion that someone is or has been involved in webcam sex tourism with real minors, which would then provide the legal basis for further investigating the suspect using other, more traditional investigative methods. The legitimacy of such an approach is very much dependent on the circumstances of the case and the criminal procedure law of the individual jurisdiction and would also require careful deliberation.

8.2 Criminal procedure law issues

If the use of Sweetie is possible in light of substantive criminal law, its application will also raise criminal procedure law questions. We have identified these two main questions:

1) Is the use of Sweetie in accordance with the law?
2) Does Sweetie respect fair trial principles in the pre-trial phase, more specifically the rules on entrapment?

Use of Sweetie in accordance with the law

Sweetie is an innovative investigation tool that actually combines three distinct investigative functions into one package, namely: 1) a lure (comparable to for instance a bait car), 2) an (undercover) agent that can engage in conversation with a suspect, 3) a device that can record information such as conversations, pictures and videos. The hybrid nature of Sweetie raises questions whether its application is in accordance with the law. We have established that Sweetie can infringe on the privacy of the suspect. As such, in most if not all of the jurisdictions under examination, criminal procedure law that provide procedural safeguards must govern the use of Sweetie.

In order for Sweetie to be applied legitimately, there must a legal basis that is sufficiently accessible and foreseeable. This means that either a specific legal basis for the use of Sweetie must be established in the law of criminal procedure (which is not the case in the jurisdictions examined), or its use must be covered by existing investigative powers and practices such as those on systematic observation, undercover work and the recording of confidential information and communication. As can be judged from table 7, in about half of the jurisdictions we examined, the use of Sweetie is not covered by existing legislation or it is not sufficiently clear that it is. The reasons for this are that 1) the investigative techniques employed by Sweetie may not be used for crimes related to webcam sex tourism, 2) the use of Sweetie clearly does not fit the existing powers, or 3) the existing powers might be usable, but there is no legal precedent.

Clearer rules on the application of Sweetie for investigative purposes will serve both the interest of legal certainty and those of effective law enforcement. By providing more clarity on the legal status of Sweetie, either through legislation, or by testing its legality in court, the proper balance can be found between protecting children and the rights of potential suspects.

Entrapment

Sweetie can be used for the non-targeted and targeted luring of suspects. Basically, the use of Sweetie starts out in a non-targeted form (i.e. Sweetie is a passive ‘lure’ in a chatroom) and moves to a targeted form (once Sweetie is solicited, she interacts directly with the suspect). Whether these forms of engaging with suspects are legitimate is dependent on the circumstances of the case. Using article 6 ECHR (fair trial) as a point of departure, we have examined the legality of Sweetie from this perspective.

When it comes to non-targeted entrapment it is important that Sweetie does not alter the existing circumstances (i.e. the chatroom and public chat) in such a way that it provides an opportunity to potential perpetrators that would not have otherwise presented itself.

Furthermore, depending on the jurisdiction law enforcement must substantiate that area is a crime hotspot and/or that they have a reasonable suspicion that the crime under investigation is taking place in that area.

When it comes to targeted entrapment it is important that Sweetie does not incite or entice the suspect to commit acts that were not already his/her intention. More specifically the chat script of Sweetie must –amongst others- adhere to the following rules: 1) Sweetie may not propose webcam sex herself, or steer the suspect in that direction, 2) Sweetie may not appeal to the suspect's conscience (e.g. telling the suspect she is a poor kid and needs the money), 3) if a suspect backs down, she may not re-engage the suspect.

8.3 Jurisdiction

Since webcam sex tourism is a global phenomenon, cross-border investigations are part and parcel of combating webcam sex tourism. This inevitably leads to jurisdictional issues. When it comes to prescriptive jurisdiction, we mainly see a difference between the examined jurisdictions in terms of criminalisation. The global fight against webcam sex tourism would benefit from more harmonisation of substantive criminal law. On the whole though, we do not expect significant issues with prescriptive jurisdiction in terms of crime and penalty havens nor susbstantial issues surrounding double criminality and mutual legal assistance.

When it comes to enforcement jurisdictions the issues are potentially bigger. We have found that there are significant differences in terms of the regulation of investigative powers throughout the different jurisdictions. In particular, the rules on the use of undercover agents differ from jurisdiction to jurisdiction. This might lead to issues when Sweetie is used extra-territorially, for instance, using Sweetie from the United States in order to catch Dutch webcam sex offenders. Addressing the issue of enforcement jurisdiction and the (unilateral) extra-territorial application of enforcement powers is no small matter. It is therefore more practical to use Sweetie mainly in a domestic context. In other words, using Sweetie only to catch national subjects, not foreigners. Another option is to use the existing mutual legal assistance procedures and to hand over investigations to local law enforcement of suspects' countries.

9 Bibliography

Books

Ashworth, A and Horder, J 2013, *Principles of criminal law*, Oxford University Press, Oxford

Ballin, MFH 2012, *Anticipative Criminal Investigation*, T.M.C. Press, the Hague

Bielefeldt, H 2012 'Philosophical and Historical Foundations of Human Rights' in C Krause & M Scheinin, (eds), *International Protection of Human Rights: A Textbook*, pp. 3 – 18, Åbo Akademi University Institute for Human Rights, Åbo

Casey, E 2011 'Foundations of Digital Forensics' in E Casey (ed), *Digital Evidence and Computer Crime*, pp. 3 – 34, Elsevier, London

Ferrante, M 2010 'Argentina' in K Heller & M Dubber, (eds), *The handbook of comparative criminal law,* pp. 12 – 48, Stanford University Press, Stanford

Goldstein, RD 1999, *Child abuse and neglect: Cases and materials: Cases and Materials (American Casebook Series)*, West Group

Gómez-Jara, C and Chiesa, L E 2010 'Spain' in K Heller & M Dubber, (eds), *The handbook of comparative criminal law,* pp. 488 – 530, Stanford University Press, Stanford

Harris, D 2010, *Cases and Materials on International Law*, Sweet & Maxwell, London

Klabbers, J 2013, *International Law*, Cambridge University Press, Cambridge

Robinson, PH 2010, 'United States' in K Heller & M Dubber, (eds), *The handbook of comparative criminal law*, pp. 563 – 592, Stanford University Press, Stanford

Ryngaert, C 2015, *Jurisdiction in International Law*, Oxford University Press, Oxford

Shaw, MN 2014, *International Law*, Cambridge University Press, Cambridge

Articles

August, R 2002, 'International Cyber-Jurisdiction: A Comparative Analysis', *American business law journal*, *39*(4), pp. 531-574.

Bellia, PL 2001, 'Chasing bits across borders' in *University of Chicago Legal Forum*, pp. 35-101.

Brenner, SW & Koops, BJ 2004, 'Approaches to Cybercrime Jurisdiction', *Journal of High Technology Law*, *4*(1), pp. 189-202.

Bronitt, S 2004, 'The law in undercover policing: A comparative study of entrapment and covert interviewing in Australia, Canada and Europe', *Common Law World Review*, *33*(1), pp. 35-80.

Georgieva, I 2015, 'The Right to Privacy under Fire Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR', *Utrecht Journal of International & European Law*, *31*, pp. 104-130.

Gillespie, AA 2012, 'Jurisdictional issues concerning online child pornography', *International Journal of Law and Information Technology*, *20*(3), pp. 151-177.

Van Hock, AA and Luchtman, MJ 2005, 'Transnational cooperation in criminal matters and the safeguarding of human rights', *Utrecht Law Review*, *1*, pp. 1-39.

Johnson, DR and Post, D 1996, 'Law and borders: The rise of law in cyberspace', *Stanford Law Review*, pp. 1367-1402.

Koops, BJ 2013, 'Police investigations in Internet open sources: Procedural-law issues', *Computer Law & Security Review*, *29*(6), pp. 654-665.

Lovejoy, TP 2007, 'A New Playground: Sexual Predators and Pedophiles Online: Criminalizing Cyber Sex between Adults and Minors', *St. Thomas Law Review*, *20*, pp. 311-358.

Slobogin, C 2012, 'Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory', *Duke Journal of Constitutional Law & Public Policy, Forthcoming*, pp.12-22.

Taslitz, AE 2013, 'Cybersurveillance without Restraint: The Meaning and Social Value of the Probable Cause and Reasonable Suspicion Standards in Governmental Access to Third-Party Electronic Records', *Journal of Criminal Law & Criminology*, *103*, pp.839-905.

Vendius, TT 2015, 'Proactive Undercover Policing and Sexual Crimes against Children on the Internet', *European Review of Organised Crime*, *2*, pp.6-24.

Wilborn, S E 1997, 'Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace', *Georgia Law Review*, *32*, p.825-888.

Williams, SA 1991, 'The Double Criminality Rule and Extradition: A Comparative Analysis', *Nova Law Review*, *15*, p.581-623.

Reports and Manuals

Committee of Ministers of the Council of Europe 2001, *Explanatory report to the Convention on Cybercrime*. *CETS Nr. 185*, Budapest

Committee of Ministers of the Council of Europe 2007, *Explanatory report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. CETS 201*, Lanzarote

Committee on the Rights of the Child 2011, *General comment No. 13: The right of the child to freedom from all forms of violence*, CRC/C/GC/13

Interagency Working Group on the Sexual Exploitation of Children 2016, *Terminology guidelines for the protection of children from sexual exploitation and sexual abuse*, Luxembourg

Kilkelly, U 2003, *A guide to the implementation of Article 8 of the European Convention on Human Rights. Human rights handbooks, No. 1*, Strasbourg

Koops, BJ and Goodwin, M 2014, *Cyberspace, the cloud, and cross-border investigation: The limits of international law*

United Nations Office on Drugs and Crime 2013, *Comprehensive study on cybercrime*, Vienna

Country reports

Argentina: Salt, M and Dupuy, D, *Substantive and procedural legislation in Argentina to combat webcam-related child sexual abuse*, May 2016

Australia: Urbas, G, *Substantive and procedural legislation in Australia to combat webcam-related child sexual abuse*, April 2016

Belgium: Royer, S, Marlier, G and Conings, C, *Substantive and procedural legislation in Belgium to combat webcam-related child sexual abuse*, updated July 2016

Brazil: Mendes Saldanha, P, *Substantive and procedural legislation in Brazil to combat webcam-related child sexual abuse*, updated May 2016

Canada: Hodge, R, *Substantive and procedural legislation in Canada to combat webcam-related child sexual abuse*, updated June 2016

Croatia: Bojić, I, *Substantive and procedural legislation in the Republic of Croatia to combat webcam-related child sexual abuse*, updated May 2016

England & Wales: Gillespie, AA, *Substantive and procedural legislation in England & Wales to combat webcam-related child sexual abuse*, March 2016

Estonia: Kala, K, *Substantive and procedural legislation in Estonia to combat webcam-related child sexual abuse*, updated May 2016

Germany: Hakobyan, H, *Webcam sex with (virtual) children: Legislative gaps or criminalised conduct? A legal analysis of Sweetie 2.0 under German substantive criminal law*

Israel: Harduf, A, *Substantive and procedural legislation in Israel to combat webcam-related child sexual abuse*, May 2016

The Netherlands: Schermer, BW, Koops, BJ and Van Der Hof, S, *Substantive and procedural legislation in the Netherlands to combat webcam-related child sexual abuse*

Nigeria: Orji, UJ, *Substantive and procedural legislation in Nigeria to combat webcam-related child sexual abuse*, updated June 2016

The Philippines: Dizon, MA, *Substantive and procedural legislation in the Philippines to combat webcam-related child sexual abuse*, updated May 2016

Poland: Skorvanek, I, *Substantive and procedural legislation in Poland to combat webcam-related child sexual abuse*, May 2016

Scotland: Richardson, A, Kerr, M and Keane, E, *Substantive and procedural legislation in Scotland to combat webcam-related child sexual abuse*, May 2016

Spain: Agustina, JR and Valverde, R, *Substantive and procedural legislation in Spain to combat webcam-related child sexual abuse*, May 2016

South Korea: Park, YC, *Substantive and procedural legislation in South Korea to combat webcam-related child sexual abuse*, July 2016

Turkey: Önok, M and Bayamlıoğlu, E, *Substantive and procedural legislation in Turkey to combat webcam-related child sexual abuse*, June 2016

USA: Unikowski, J, *Substantive and procedural legislation in United States of America to combat webcam-related child sexual abuse*, May 2016

Legal Instruments

Convention for the Protection of Human Rights and Fundamental Freedoms, CETS no. 194, Rome, 4.XI.1950

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171

Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3

Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (adopted on 25 May 2000, entered into force 18 January 2002) A/RES/54/263

Council of Europe Convention on Cybercrime, CETS No.185, Budapest, 23.XI.2001

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS 201, Lanzarote, 25.X.2007

Parliament and Council Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters

Case law

Australia:

Britten v Alpogut [1987] VR 929

Ridgeway v The Queen [1995] CLR 19

O'Neill v R [1995] 81 A Crim R 458

McEwewn v Simmons & Anor [2008] NSWSC 1292

R v Priest [2011] ACTSC 18

Belgium:

Brussel 14 maart 2007, *RABG* 2008

Cass. 17 maart 2010, AR P100010F

Canada:

R v Mack [1988] 2 SCR 903

R v Alicandro [2009] ONCA 133 (CanLII)

R v Spencer [2014] 2 SCR 212, 2014 SCC 43 (CanLII)

Croatia:

VSRH, I Kž-1255/04 of 16 February 2006

(Judgement of the Supreme Court)

ECtHR:

Handyside v the UK, Application no. 5493/72, judgment of 7 December 1976

Klass and others v Germany, Application no. 5029/71, judgement of 6 September 1978

Dudgeon v the UK, Application no. 7525/76, judgment of 22 Oct. 1981
Leander v Sweden, Application no. 9248/81, judgement of 26 March 1987
Olsson v Sweden, Application no. 10465/83, judgment of 24 March 1988
Texeira do Castro v Portugal, Application nos. 44/1997/828/1034, judgement of 9 June 1998
Halford v the UK, Application no. 44787/98, judgement of 25 September 2001
Peck v the UK, Application no. 44647/98, judgement of 28 January 2003
Shannon v the UK, Application no. 67537/01, admissibility decision of 6 April 2004
Von Hannover v Germany [GC], Application no. 59320/00, judgement of 24 June 2004
Weber and Saravia v Germany, Application no. 54934/00, judgement of 29 June 2006
Ramanauskas v Lithuania [GC], Application no. 74420/01, judgement of 5 February 2008
Malininas v Lithuania, Application no. 10071/04, judgement of 1 October 2008
KU v Finland, Application no. 2872/02, judgement of 2 December 2008
Constantin and Stoian v Romania, Applications no. 23782/06 and 46629/06, judgement of 29 December 2009
Burak Hun v Turkey, Application no. 17570/04, judgement of 15 March 2010
Bannikova v Russia, Application no. 18757/06, judgement of 4 February 2011

England and Wales:
Haughton v Smith [1975] AC 476

Estonia:
RKKKo 3-1-1-110-04
(Judgment of the Supreme Court of 2 December 2004, case number 3-1-1-110-04)

Israel:
Ktiei v Israel, LCrimA 1201/12 [9 January 2014]

The Netherlands:
HR 4 December 1979, NJ 1980, 356 m.nt ThWvV
HR 30 Nov 2004, ECLI:NL:HR:2004:AQ0950
HR 28 Oct 2008, ECLI:NL:HR:2008:BE9817
HR 6 Oct 2009, ECLI:NL:HR:2009:BI7084
(Supreme Court Judgements)

Rb. Groningen 16 October 2003, LJNAM1882, case no. 18/076010-01

Rb. Alkmaar 19 February 2004, LJNA05509, case no. 14.060137-02

The Philippines:

Araneta v Court of Appeals, G.R. No. L-46638 [9 July 1986]

People v Gatong-o, G.R. No. 78698 [29 December 1988]

Scotland:

Docherty v Brown [1996] JC 48

Jones v HM Advocate [2009] HCJAC 86

South Korea:

2008DO7362, Oct. 23, 2008

(Judgement of the Supreme Court)

Spain:

Judgement of the Supreme Court of Justice 300/2015, of 19 May (Spain)

SSCS June 22, 1950

SSCS April 18, 1972

SSCS February 16, 2007, available at www.westlaw.es, Ref: RJ 2007\2381.

United States*:*

Lopez v United States, 373 U.S. 427 (1963)

Hoffa v United States, 385 U.S. 293 (1966)

Katz v United States, 389 U.S. 347 (1967)

United States v Miller, 425 U.S. 435 (1976)

Smith v Maryland, 442 U.S. 735 (1979)

Mathews v United States, 485 U.S. 58 (1988)

Alabama v White, 496 U.S. 325 (1990)

State *v* Moretti, 244 A.2d 499 (N.J. 1968)

United States v Gorshkov, No CR00-500C (W D Wash May 23, 2001)

United States v Jackson, 488 F. Supp. 2d 866 (D. Neb. 2007)